Manuale dell'utente

Allen-Bradley

Controllori GuardLogix 5570

Numeri di catalogo 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT, 1756-L72EROMS

Studio 5000 Automation Engineering & Design Environment

Traduzione delle istruzioni originali

Informazioni importanti per l'utente

Prima di installare, configurare, utilizzare o della manutenzione di questo prodotto, leggere il presente documento e i documenti elencati nella sezione delle ulteriori risorse riguardanti l'installazione, la configurazione e il funzionamento della macchina. Oltre ai requisiti previsti dalle normative, dalle leggi e dagli standard vigenti, gli utenti sono tenuti a conoscere le istruzioni di installazione e di cablaggio.

Attività quali l'installazione, la regolazione, la messa in servizio, l'uso, l'assemblaggio, lo smontaggio e la manutenzione devono essere eseguite da personale opportunamente formato secondo quanto previsto dai codici professionali vigenti.

Se l'apparecchiatura viene utilizzata per uso diverso da quello specificato dal produttore, i sistemi di protezione dell'apparecchiatura potrebbero essere compromessi.

Rockwell Automation, Inc. declina qualsiasi responsabilità per danni indiretti derivanti dall'utilizzo o dall'applicazione di questa apparecchiatura.

Gli esempi e gli schemi contenuti nel presente manuale sono inclusi solo a scopo illustrativo. Poiché le variabili e i requisiti associati alle installazioni specifiche sono innumerevoli, Rockwell Automation, Inc. non può essere ritenuta responsabile per l'utilizzo effettivo basato sugli esempi e sugli schemi qui riportati.

Rockwell Automation, Inc. declina qualsiasi responsabilità brevettuale riguardo all'utilizzo di informazioni, circuiti, apparecchiatura o software descritti nel presente manuale.

È vietata la riproduzione, parziale o integrale, del contenuto di questo manuale senza previo consenso scritto di Rockwell Automation, Inc.

All'interno del presente manuale, quando necessario, sono inserite note destinate a richiamare l'attenzione dell'utente su argomenti riguardanti la sicurezza.

	AVVERTENZA: indica informazioni su procedure o circostanze che possono provocare un'esplosione in un ambiente pericoloso che potrebbe comportare lesioni personali o morte, nonché danni materiali o economici.
	ATTENZIONE: Indica informazioni sulle pratiche o le circostanze che possono causare lesioni personali o morte, danni alle proprietà o perdite economiche. I simboli di attenzione consentono di identificare o evitare un pericolo e di riconoscerne le conseguenze.
IMPORTANTE	Indica le informazioni indispensabili per l'applicazione corretta e la comprensione del prodotto.

Delle etichette con precauzioni specifiche potrebbero trovarsi anche all'esterno o all'interno dell'apparecchiatura.

	PERICOLO DI FOLGORAZIONE: queste etichette possono essere apposte sopra o all'interno dell'apparecchiatura, ad esempio su un servoazionamento o un motore, per avvertire della presenza di tensione pericolosa.
	PERICOLO DI USTIONI: Queste etichette possono essere apposte sopra o all'interno dell'apparecchiatura, ad esempio su un servoazionamento o un motore, per segnalare che le superfici possono raggiungere temperature pericolose.
	PERICOLO DI ARCO ELETTRICO: Queste etichette possono trovarsi all'esterno o all'interno dell'apparecchiatura, ad esempio su un motor control center per avvisare gli utenti di un potenziale rischio di arco elettrico. Gli archi elettrici possono causare lesioni gravi o mortali. Indossare dispositivi di protezione individuale (DPI) appropiati. Rispettare TUTTI i requisiti normativi sulle pratiche di lavoro sicure e sui dispositivi di protezione individuale (DPI).

Allen-Bradley, Armor, ControlFLASH, ControlLogix, DriveLogix, FlexLogix, Guard I/O, GuardLogix, Architettura Integrata, Kinetix, Logix5000, PanelView, PhaseManager, PLC-5, POINT Guard I/O, PowerFlex, Rockwell Automation, Rockwell Software, RSLinx, RSLogix, RSNetWorx, Studio 5000, Studio 5000 Automation Engineering & Design Environment e Studio 5000 Logix Designer sono marchi commerciali di Rockwell Automation, Inc.

ControlNet, DeviceNet ed EtherNet/IP sono marchi commerciali di ODVA. I marchi commerciali che non appartengono a Rockwell Automation sono di proprietà delle rispettive società.

Questo manuale contiene informazioni nuove e aggiornate.

Informazioni nuove e aggiornate

Questa tabella contiene le modifiche apportate a questa versione.

Argomento	Pagina
Titolo di sezione cambiato da "Altre risorse" a "Per ulteriori informazioni".	11
Descrizione della colonna delle risorse cambiata da "Servoazionamenti Kinetix®" a "Servoazionamenti".	12
"Kinetix 5700 Servo Drives User Manual" e "PowerFlex® 527 Adjustable Frequency AC Drive User Manual" aggiunti al materiale di riferimento per i servoazionamenti.	12
Informazioni relative a versioni precedenti rimosse dalla tabella "Funzioni supportate".	19
Titolo della colonna modificato da "Versione 24" a "Versione 24 e successive".	19
Frase introduttiva e Figura 10 aggiunte al manuale.	48
Contenuto di assegnazione SNN aggiunto alla tabella "Importante".	49
Figura 14 rivista in modo da includere i convertitori di frequenza PowerFlex 527 e i servoazionamenti Kinetix 5700.	56
Convertitori di frequenza PowerFlex 527 e servoazionamenti Kinetix 5700 aggiunti alle relative informazioni di indirizzo.	73
Titolo e informazioni della Tabella 20 rivisti in modo da includere più convertitori di frequenza e servoazionamenti.	73
Convertitori di frequenza PowerFlex 527 e servoazionamenti Kinetix 5700 aggiunti come ulteriori informazioni di riferimento.	74

Note:

Prefazione

Informazioni sui controllori GuardLogix. 9
Controllori per ambienti estremi 10
Controllori Armor GuardLogix 10
Studio 5000 10
Terminologia. 11
Per ulteriori informazioni 11

Capitolo 1

Cenni generali sul sistema

Requisiti delle applicazioni di sicurezza 13
Numero della rete di sicurezza. 13
Firma del task di sicurezza. 14
Distinzione tra componenti standard e di sicurezza 14
Dispositivi di interfaccia operatore. 14
Capacità del flusso di dati del controllore 15
Scelta dell'hardware del sistema 16
Controllore primario 16
Coprocessore di sicurezza 17
Chassis 17
Alimentatore 17
Scelta dei dispositivi I/O di sicurezza 17
Scelta delle reti di comunicazione 18
Requisiti di programmazione 18

Capitolo 2

Installazione del controllore

Precauzioni. 21
Informazioni ambientali e sulla custodia 21
Sistemi elettronici programmabili (PES, Programmable Electronic Systems) 22
Rimozione e inserimento sotto tensione (RIUP, Removal and Insertion Under Power) 22
Approvazione nordamericana per l'uso in aree pericolose 22
Approvazione europea per aree pericolose 23
Prevenzione delle scariche elettrostatiche. 23
Verificare di avere tutti i componenti 24
Installazione di un alimentatore e di uno chassis 25
Installazione del controllore nello chassis. 25
Inserimento o rimozione di una scheda di memoria 26
Rimozione della scheda SD 27
Installazione della scheda SD 28
Collegamenti di comunicazione 29
Aggiornamento del controllore. 31
Utilizzo del software ControlFLASH per l'aggiornamento del firmware 31
Utilizzo di AutoFlash per l'aggiornamento del firmware 32
Scelta della modalità operativa del controllore 33
Uso del selettore a chiave per cambiare la modalità operativa 33
Utilizzo dell'applicazione Logix Designer per cambiare la modalità operativa 34
Disinstallazione del modulo di alimentazione (ESM) 34
Installazione di un modulo di alimentazione (ESM). 36

Capitolo 3

Configurazione del controllore

Creazione di un progetto del controllore 39
Codifica elettronica 42
Ulteriori informazioni 42
Impostazione delle -password per il blocco/sblocco di sicurezza 42
Protezione della firma del task di sicurezza in modalità Esecuzione 43
Gestione della sostituzione dei moduli I/O 44
Abilitazione della sincronizzazione temporale 45
Configurazione di un controllore di sicurezza peer 45

Capitolo 4

Comunicazione sulle reti

Rete di sicurezza 47
Gestione del numero della rete di sicurezza (SNN) 47
Assegnazione del numero di rete di sicurezza (SNN) 49
Modifica del numero di rete di sicurezza (SNN) 50
Comunicazione EtherNet/IP 53
Produzione e consumo dei dati attraverso una rete EtherNet/IP . . . 54
Connessioni sulla rete EtherNet/IP 54
Esempi di comunicazione EtherNet/IP 55
Connessioni EtherNet/IP per dispositivi I/O di sicurezza. 56
Connessioni EtherNet/IP standard 57
Comunicazione ControlNet 58
Produzione e consumo dei dati attraverso una rete ControlNet. . . . 58
Connessioni sulla rete ControlNet. 59
Esempio di comunicazione ControlNet 59
Connessioni ControlNet per I/O distribuiti. 60
Comunicazione DeviceNet 60
Connessioni DeviceNet per dispositivi I/O di sicurezza. 61
Connessioni DeviceNet standard 61

Capitolo 5

Aggiunta, configurazione, monitoraggio e sostituzione dei dispositivi I/O CIP Safety

Aggiunta di dispositivi I/O di sicurezza 63
Configurazione dei dispositivi I/O di sicurezza 64
Impostazione dell'indirizzo IP tramite il sistema di traduzione degli indirizzi di rete (NAT) 65
Impostazione del numero rete di sicurezza (SNN) 67
Utilizzo delle connessioni unicast su reti EtherNet/IP. 67
Impostazione del limite del tempo di risposta della connessione 67
Impostazione dell'intervallo di pacchetto richiesto (RPI) 67
Visualizzazione del ritardo rete massimo osservato 68
Impostazione dei parametri avanzati relativi ai limiti del tempo di risposta della connessione. 69
Comprensione dell'autenticazione di configurazione. 71
Configurazione mediante l'applicazione Logix Designer 71
Proprietario della configurazione diverso (connessione di solo ascolto) 71
Ripristino della proprietà dei dispositivi I/O di sicurezza 72
Indirizzamento dei dati I/O di sicurezza 72
Formato dell'indirizzo dei moduli I/O di sicurezza 72
Formato di indirizzo per i servoazionamenti Kinetix 5500 e Kinetix 5700 e per PowerFlex 527 73
Monitoraggio dello stato dei dispositivi I/O di sicurezza. 74

Reset di un modulo alle condizioni predefinite in fabbrica 75
Sostituzione di un dispositivo utilizzando l'applicazione Logix Designer 75
Sostituzione con l'opzione "Configure Only When No Safety Signature Exists" abilitata 76
Sostituzione con l'opzione "Configure Always" abilitata 80
Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet 81

Capitolo 6

Sviluppo di applicazioni di sicurezza

Task di sicurezza 86
Definizione del periodo del task di sicurezza 86
Esecuzione del task di sicurezza 87
Programmi di sicurezza 87
Routine di sicurezza 88
Tag di sicurezza 88
Tipo di tag 89
Tipo di dati 90
Ambito 90
Classe 91
Valore costante 92
Accesso esterno 92
Tag di sicurezza prodotti/consumati 92
Configurazione dei numeri di rete di sicurezza dei controllori di sicurezza peer 93
Produzione di un tag di sicurezza 95
Consumo di dati tag di sicurezza 96
Mappatura dei tag di sicurezza 98
Restrizioni 98
Creazione di coppie di mappatura di tag 99
Controllo dello stato della mappatura dei tag 100
Protezione dell'applicazione di sicurezza 100
Blocco di sicurezza del controllore 100
Generazione di una firma del task di sicurezza 102
Programmazione delle restrizioni 103

Capitolo 7

Collegamento online con il controllore

Connessione del controllore alla rete 105
Connessione del dispositivo EtherNet/IP e del computer 105
Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer 106
Configurazione di un driver EtherNet/IP, ControlNet o DeviceNet 106
Analisi dei fattori che influiscono sul collegamento online 106
Corrispondenza tra progetto e controllore 106
Corrispondenza della versione del firmware 107
Stato di sicurezza/errori 107
Firma del task di sicurezza e stato di blocco/sblocco di sicurezza 107
Download 108
Upload 110
Collegamento online 111

Capitolo 8

Memorizzazione e caricamento di progetti con la memoria non volatile

Utilizzo delle schede di memoria per la memoria non volatile 113
Memorizzazione di un progetto di sicurezza 114
Caricamento di un progetto di sicurezza 115
Utilizzo dei moduli di alimentazione 116
    Salvataggio del programma sulla memoria NVS integrata 116
    Cancellazione del programma dalla memoria NVS integrata 117
Valutazione dell'alimentazione dell'orologio interno (WallClockTime) da parte del modulo ESM 118
Gestione del firmware con Firmware Supervisor 118

Capitolo 9

Monitoraggio dello stato e gestione degli errori

Visualizzazione dello stato attraverso la barra online..... 119
Monitoraggio delle connessioni 120
    Tutte le connessioni 120
    Connessioni di sicurezza 121
Monitoraggio degli indicatori di stato..... 121
Monitoraggio dello stato di sicurezza 122
Errori del controllore..... 122
    Errori irreversibili del controllore 122
    Errori di sicurezza irreversibili nell'applicazione di sicurezza..... 123
    Errori reversibili nell'applicazione di sicurezza 123
    Visualizzazione degli errori..... 123
    Codici di errore 124
Sviluppo di una routine di errore 124
    Routine di errore del programma 125
    Gestore degli errori del controllore..... 125
    Utilizzo delle istruzioni GSV/SSV 125

Appendice A

Indicatori di stato

Indicatori di stato dei controllori 129
Display dello stato del controllore 130
    Messaggi di stato di sicurezza 130
    Messaggi di stato generali 131
    Messaggi di errore 132
    Messaggi relativi agli errori gravi reversibili 133
    Codici di errore I/O 134

Appendice B

Modifica del tipo di controllore

Cambio da controllore standard a controllore di sicurezza 137
Cambio da controllore di sicurezza a controllore standard 138
Cambio del tipo di controllore di sicurezza..... 138
Altre risorse 139

Argomento	Pagina
Informazioni sui controllori GuardLogix	9
Studio 5000	10
Terminologia	11
Per ulteriori informazioni	11

Questo manuale è una guida per l'utilizzo di un controllore GuardLogix® 5570 in un'applicazione Studio 5000 Logix Designer™. Vengono descritte le procedure specifiche per GuardLogix utilizzate per la configurazione, l'uso e la ricerca guasti sul controllore.

Utilizzare questo manuale se si è responsabili della progettazione, l'installazione, la programmazione o la ricerca dei guasti relativi ai sistemi di controllo che impiegano i controllori GuardLogix 5570.

È necessario avere una conoscenza di base dei circuiti elettrici ed esperienza con la logica a relè. È inoltre necessario avere la formazione e l'esperienza necessarie per la creazione, l'utilizzo e la manutenzione dei sistemi di sicurezza.

Per informazioni dettagliate su argomenti correlati al controllore GuardLogix, i requisiti per il livello di integrità della sicurezza (SIL) 3 e i livelli di prestazioni (e) (SIL 3/PLe) o per informazioni sui componenti Logix standard, consultare l'elenco Per ulteriori informazioni a pagina 11.

Informazioni sui controllori GuardLogix

Sono disponibili due linee di controllori GuardLogix 1756. Questi controllori condividono molte funzioni, ma hanno anche qualche differenza. La Tabella 1 spiega brevemente tali differenze.

Tabella 1 - Differenze tra controllori GuardLogix 5570 e GuardLogix 5560

Funzione	**Controllori GuardLogix 5570** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**Controllori GuardLogix 5560** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Supporto dell'orologio e backup per il mantenimento della memoria allo spegnimento	Modulo di alimentazione (ESM, Energy storage module)	Batteria
Porte di comunicazione (integrate)	USB	Seriale
Connessioni, controllore	500	250
Memoria, non volatile	Scheda Secure Digital (SD)	Scheda CompactFlash (CF)
Indicatori di stato	Display dello stato a scorrimento e indicatori di stato	Indicatori di stato
Strumento di programmazione	Studio 5000, versione 21 o successiva Software RSLogix™ 5000, versione 20 o successiva	Software RSLogix 5000, versione 14 Software RSLogix 5000, versione 16 o successiva
Manuale d'uso	• Ambiente Studio 5000: questo manuale • Software RSLogix 5000: 1756-UM020	1756-UM020
Manuale di riferimento per la sicurezza	• Ambiente Studio 5000: 1756-RM099 • Software RSLogix 5000: 1756-RM093	1756-RM093

Controllori per ambienti estremi

I controllori GuardLogix per ambienti estremi, numeri di catalogo 1756-L73SXT e 1756-L7SPXT, forniscono le stesse funzionalità del controllore 1756-L73S, ma sono progettati per sopportare temperature comprese nel campo –25...70 °C.

IMPORTANTE	I componenti del sistema Logix-XT sono idonei a condizioni ambientali estreme solo se utilizzati correttamente con altri componenti del sistema Logix-XT. L'utilizzo di componenti Logix-XT con componenti del sistema Logix tradizionale compromette l'idoneità all'impiego in ambienti estremi.

Controllori Armor GuardLogix

Il controllore Armor™ GuardLogix (numero di catalogo 1756-L72EROMS) è la combinazione di un controllore 1756-L72S GuardLogix e di un coprocessore di sicurezza con due canali di comunicazione Ethernet/IP™ compatibili con la topologia DLR in una custodia IP67 per il montaggio su macchina. Per ulteriori informazioni sul controllore Armor GuardLogix consultare le Istruzioni per l'installazione Controllore Armor GuardLogix, pubblicazione 1756-IN060B-IT-P.

Studio 5000

Studio 5000 Automation Engineering & Design Environment™ combina elementi di sviluppo e progettazione in un ambiente comune. Il primo elemento di Studio5000 è l'applicazione Logix Designer. L'applicazione Logix Designer è il nuovo nome del software RSLogix 5000 e continua ad essere il prodotto destinato alla programmazione dei controllori Logix5000™ per soluzioni di controllo discreto, di processo, batch, controllo assi, sicurezza e basate su servoazionamenti.

L'ambiente Studio 5000 è la base per le future versioni degli strumenti e delle funzioni di sviluppo di Rockwell Automation®. L'ambiente Studio 5000 è l'unico strumento di lavoro che consente ai progettisti di sviluppare tutti gli elementi del loro sistema di controllo.

Terminologia

Nella seguente tabella sono riportate le definizioni dei termini utilizzati nel presente manuale.

Tabella 2 - Termini e definizioni

Abbreviazione	Termine completo	Definizione
1oo2	One Out of Two (Uno di due)	Si riferisce alla progettazione comportamentale di un sistema di sicurezza a più processori.
CIP	Common Industrial Protocol	Protocollo di comunicazione progettato per le applicazioni di automazione industriale.
CIP Safety	Common Industrial Protocol – Safety Certified	Versione SIL 3/PLe del protocollo CIP.
CD	Copertura diagnostica	Il rapporto tra tasso di guasto rilevato e tasso di guasto totale.
EN	European Norm	Norme ufficiali europee.
ESM	Modulo di alimentazione	Utilizzato per il supporto dell'orologio e il backup della memoria allo spegnimento sui controllori GuardLogix 5570.
GSV	Get System Value	Istruzione che recupera le informazioni specificate relative allo stato del controllore e le posiziona in un tag di destinazione.
—	Multicast	Trasmissione delle informazioni da un trasmettitore a più ricevitori.
NAT	Network Address Translation	Trasformazione di un indirizzo Internet Protocol (IP) in un altro indirizzo IP su un'altra rete.
PFD	Probabilità di guasto su domanda	La probabilità media di un sistema di non adempiere alla sua funzione di progetto su domanda.
PFH	Probabilità di guasto all'ora	La probabilità per un sistema di subire un guasto pericoloso all'ora.
PL	Livelli prestazionali	Classe di sicurezza ISO 13849-1.
RPI	Intervallo di pacchetto richiesto	Durante la comunicazione su una rete, l'intervallo previsto di produzione dati.
SNN	Safety Network Number	Un numero univoco che identifica una sezione della rete di sicurezza.
SSV	Set System Value	Istruzione che imposta i dati del sistema del controllore.
—	Standard	Un oggetto, task, tag, programma o componente del progetto non relativo alla sicurezza.
—	Unicast	Trasmissione delle informazioni da un trasmettitore ad un ricevitore.

Per ulteriori informazioni

Questi documenti contengono altre informazioni relative ai prodotti Rockwell Automation collegati.

Tabella 3 - Pubblicazioni correlate ai sistemi e ai controllori GuardLogix

Risorsa		Descrizione
Requisiti delle applicazioni di sicurezza	Manuale di riferimento per la sicurezza - Sistemi di controllo GuardLogix 5570, pubblicazione 1756-RM099B-IT-P	Contiene requisiti dettagliati per ottenere e mantenere il livello SIL 3/PLe con il sistema di controllo GuardLogix 5570, utilizzando l'applicazione Logix Designer in Studio 5000.
	GuardLogix Controller Systems Safety Reference Manual, pubblicazione 1756-RM093	Contiene requisiti dettagliati per ottenere e mantenere il livello SIL 3/PLe con il sistema del controllore GuardLogix 5560 o 5570, utilizzando il software RSLogix 5000.
CIP Sync (sincronizzazione temporale)	Integrated Architecture® and CIP Sync Configuration Application Technique, pubblicazione IA-AT003	Fornisce informazioni dettagliate e complete sulle modalità di applicazione della tecnologia CIP Sync per sincronizzare gli orologi in un sistema di controllo Logix.
Moduli Guard I/O™	Manuale dell'utente Moduli di sicurezza Guard I/O DeviceNet, pubblicazione 1791DS-UM001J-IT-P	Fornisce informazioni sull'utilizzo dei moduli Guard I/O DeviceNet Safety.
	Guard I/O EtherNet/IP Safety Modules User Manual, pubblicazione 1791ES-UM001	Fornisce informazioni sull'uso dei moduli Guard I/O EtherNet/IP Safety.
	Manuale dell'utente Moduli di sicurezza POINT Guard I/O™, pubblicazione 1734-UM013B-IT-P	Fornisce informazioni sulle procedure di installazione, configurazione e uso dei moduli POINT Guard I/O.
	Istruzioni per l'installazione Controllore Armor GuardLogix, pubblicazione 1756-IN060B-IT-P.	Fornisce informazioni sull'installazione e l'uso dei controllori Armor GuardLogix.

Tabella 3 - Pubblicazioni correlate ai sistemi e ai controllori GuardLogix (segue)

Risorsa		Descrizione
Servoazionamenti	Manuale dell'utente Servoazionamenti Kinetix 5500, pubblicazione 2198-UM001A-IT-P	Fornisce informazioni sull'installazione, la configurazione, l'avviamento e la ricerca guasti del sistema di servoazionamenti Kinetix 5500. Contiene anche i requisiti per utilizzare i servoazionamenti Kinetix 5500 nelle applicazioni di sicurezza.
	Kinetix 5700 Servo Drives User Manual, pubblicazione 2198-UM002	Fornisce informazioni sull'installazione, la configurazione, l'avviamento e la ricerca guasti del sistema di servoazionamenti Kinetix 5700. Contiene anche i requisiti per utilizzare i servoazionamenti Kinetix 5700 nelle applicazioni di sicurezza.
	PowerFlex 527 Adjustable Frequency AC Drive User Manual, pubblicazione 520-UM002	Fornisce informazioni sull'installazione, l'avviamento e la risoluzione dei problemi del convertitore di frequenza PowerFlex serie 520.
Installazione hardware	Chassis e alimentatore ControlLogix®, Istruzioni per l'installazione, pubblicazione 1756-IN005C-IT-P	Spiega come installare e mettere a terra gli alimentatori e lo chassis ControlLogix.
	Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1	Fornisce informazioni dettagliate su come mettere a terra e collegare i controllori programmabili.
Istruzioni (programmazione)	GuardLogix Safety Application Instruction Set Reference Manual, pubblicazione 1756-RM095	Fornisce informazioni sul set di istruzioni dell'applicazione di sicurezza GuardLogix.
	Manuale di riferimento Istruzioni generali per controllori Logix5000, pubblicazione 1756-RM003K-IT-P	Fornisce ai programmatori i dettagli su tutte le istruzioni disponibili per un controllore Logix5000.
	Logix5000 Controllers Motion Instructions Reference Manual, pubblicazione MOTION-RM002	Fornisce ai programmatori tutti i dettagli sulle istruzioni di controllo assi disponibili per un controllore Logix5000.
Controllo assi	Sercos Motion Configuration and Startup User Manual, pubblicazione MOTION-UM001	Spiega come configurare un sistema applicativo di controllo assi SERCOS.
	Motion Coordinated Systems User Manual, pubblicazione MOTION-UM002	Spiega come creare e configurare un sistema applicativo di controllo assi coordinato.
	Manuale dell'utente Configurazione ed avvio di Integrated Motion su Ethernet/IP, pubblicazione MOTION-UM003D-IT-P	Spiega come configurare un sistema applicativo Integrated Motion su reti EtherNet/IP.
	Integrated Motion on the EtherNet/IP Network Reference Manual, pubblicazione MOTION-RM003	Informazioni dettagliate sulle modalità di controllo assi e sugli attributi per Integrated Motion su reti EtherNet/IP.
Reti (ControlNet™, DeviceNet, EtherNet/IP)	Moduli EtherNet/IP in sistemi di controllo Logix5000 Manuale dell'utente, pubblicazione ENET-UM001L-IT-P	Spiega come configurare ed utilizzare i moduli EtherNet/IP in un sistema di controllo Logix5000.
	ControlNet Modules in Logix5000 Control Systems User Manual, pubblicazione CNET-UM001	Spiega come configurare e utilizzare i moduli ControlNet in un sistema di controllo Logix5000.
	DeviceNet Modules in Logix5000 Control Systems User Manual, pubblicazione DNET-UM004	Spiega come configurare e utilizzare i moduli DeviceNet in un sistema di controllo Logix5000.
PhaseManager™	PhaseManager User Manual, pubblicazione LOGIX-UM001	Fornisce procedure, guida ed esempi per la configurazione e la programmazione di un controllore Logix5000 per l'uso delle fasi di apparecchiatura.
Procedure e task di programmazione	Logix5000 Controllers Common Procedures Programming Manual, pubblicazione 1756-PM001	Consente di accedere alla serie di manuali di programmazione per i controllori Logix5000, contenenti informazioni su argomenti quali la gestione dei file di progetto, l'organizzazione dei tag, la logica di programma, la verifica delle routine, la gestione degli errori ecc.
	Logix5000 Controllers Execution Time and Memory Use Reference Manual, pubblicazione 1756-RM087	Fornisce informazioni su come stimare l'uso della memoria e il tempo d'esecuzione della logica programmata e su come scegliere tra le varie opzioni di programmazione.

Per consultare o scaricare le pubblicazioni, visitare il sito http://www.rockwellautomation.com/literature. Per ordinare una copia cartacea della documentazione tecnica, contattare il distributore Allen-Bradley® o il rappresentante di vendita locale Rockwell Automation.

Cenni generali sul sistema

Argomento	Pagina
Requisiti delle applicazioni di sicurezza	13
Distinzione tra componenti standard e di sicurezza	14
Capacità del flusso di dati del controllore	15
Scelta dell'hardware del sistema	16
Scelta dei dispositivi I/O di sicurezza	17
Scelta delle reti di comunicazione	18
Requisiti di programmazione	18

Requisiti delle applicazioni di sicurezza

Il controllore GuardLogix 5570 è certificato per l'impiego nelle applicazioni di sicurezza fino al livello di integrità della sicurezza (SIL CL, Safety Integrity Level Claim Limit) 3 e al livello prestazionale (PL, Performance Level) (e) inclusi nei quali lo stato diseccitato è lo stato di sicurezza. I requisiti delle applicazioni di sicurezza comprendono la valutazione della probabilità dei tassi di guasto, come ad esempio:

- Probabilità di guasto su domanda (PFD)
- Probabilità di guasto per ora (PFH)
- Impostazioni del tempo di risposta del sistema
- Test di verifica funzionale che soddisfano i criteri del livello SIL 3/PLe

Le applicazioni di sicurezza SIL 3/PLe basate su GuardLogix richiedono l'uso di almeno un numero della rete di sicurezza (SNN, Safety Network Number) e di una firma del task di sicurezza. Entrambi influiscono sulla configurazione di controllore e I/O e sulla comunicazione di rete.

Per informazioni sui requisiti dei sistemi di sicurezza SIL 3 e PLe, comprese le frequenze dei test di validazione funzionale, il tempo di risposta del sistema e i calcoli PFD/PFH, fare riferimento al Manuale di riferimento per la sicurezza - Sistemi di controllo GuardLogix 5570, pubblicazione 1756-RM099B-IT-P. Prima di utilizzare un sistema di sicurezza GuardLogix SIL 3, PLe è necessario leggere, comprendere e osservare questi requisiti.

Numero della rete di sicurezza

Il numero della rete di sicurezza (SNN, Safety Network Number) deve essere un numero univoco che identifica le sottoreti di sicurezza. Ogni sottorete di sicurezza utilizzata dal controllore per le comunicazioni di sicurezza deve avere un numero SNN univoco. Ogni dispositivo di sicurezza I/O deve inoltre essere configurato con il numero della rete di sicurezza (SSN) della sottorete di sicurezza. Il numero SNN può essere assegnato automaticamente o manualmente.

Per informazioni su come assegnare il numero SNN, vedere Gestione del numero della rete di sicurezza (SNN) a pagina 47.

Firma del task di sicurezza

La firma del task di sicurezza è costituita da un numero ID, dalla data e dall'ora, che identificano in modo univoco la parte di sicurezza di un progetto, compresi logica di sicurezza, dati e configurazione. Il sistema GuardLogix utilizza la firma del task di sicurezza per determinare l'integrità del progetto e per consentirvi di verificare che nel controllore di destinazione venga scaricato il progetto corretto. La possibilità di creare, registrare e verificare la firma del task di sicurezza è un passaggio obbligato del processo di sviluppo dell'applicazione di sicurezza.

Per ulteriori informazioni, vedere Generazione di una firma del task di sicurezza a pagina 102.

Distinzione tra componenti standard e di sicurezza

Gli slot di uno chassis del sistema GuardLogix non utilizzati dalla funzione di sicurezza possono essere riempiti con altri moduli ControlLogix certificati in base alle Direttive per la Bassa Tensione ed EMC. Per trovare il certificato CE relativo alla famiglia di prodotti con controllo programmabile > ControlLogix e determinare quali moduli sono certificati, vedere http://www.rockwellautomation.com/rockwellautomation/certification/ce.page.

È necessario creare e documentare una distinzione chiara, logica e visibile tra le parti standard e di sicurezza del progetto del controllore. Ai fini di questa distinzione, l'applicazione Logix Designer dispone di icone di identificazione della sicurezza per identificare task di sicurezza, programmi di sicurezza, routine di sicurezza e componenti di sicurezza. Inoltre, l'applicazione Logix Designer utilizza un attributo di classe di sicurezza visibile ogni volta che si visualizzano le proprietà di task di sicurezza, programmi di sicurezza, routine di sicurezza, tag di sicurezza o istruzioni Add-On di sicurezza.

Il controllore non consente di scrivere nei dati dei tag di sicurezza da dispositivi di interfaccia operatore (HMI) esterni o tramite le istruzioni di messaggio da controllori peer. L'applicazione Logix Designer è in grado di scrivere i tag di sicurezza quando il controllore GuardLogix è in sblocco di sicurezza, non ha una firma del task di sicurezza ed è in funzione senza errori di sicurezza.

In Sistema ControlLogix – Manuale dell'utente, pubblicazione 1756-UM001N-IT-P, sono disponibili ulteriori informazioni sull'utilizzo dei dispositivi ControlLogix in applicazioni standard (non di sicurezza).

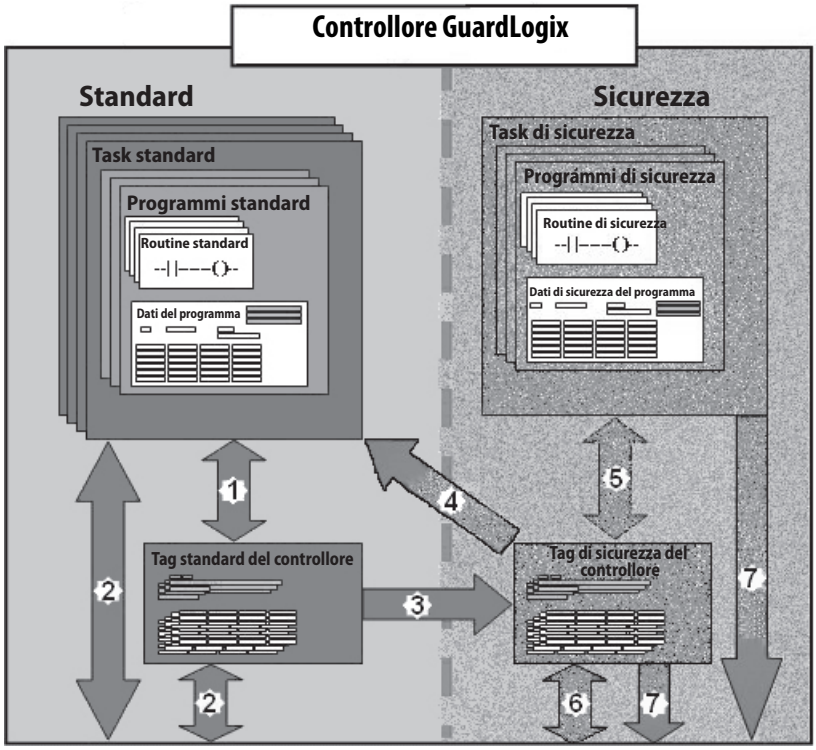
Dispositivi di interfaccia operatore

Con i controllori GuardLogix è possibile utilizzare i dispositivi di interfaccia operatore. I dispositivi di interfaccia operatore sono in grado di accedere ai tag standard come qualsiasi altro controllore standard. Tuttavia, non sono in grado di scrivere nei tag di sicurezza che, per tali dispositivi, sono di sola lettura.

Capacità del flusso di dati del controllore

La figura riportata di seguito illustra il flusso di dati standard e di sicurezza del controllore GuardLogix.

Figura 1 – Capacità del flusso di dati



Numero	Descrizione
1	I tag e la logica standard si comportano in modo identico a quanto avviene nella piattaforma Logix standard.
2	I dati di tag standard, dell'ambito del programma o del controllore, possono essere scambiati con dispositivi di interfaccia operatore, personal computer ed altri controllori esterni.
3	I controllori GuardLogix sono controllori integrati dotati della possibilità di spostare (mappare) dati da tag standard in tag di sicurezza per utilizzarli all'interno del task di sicurezza.
	ATTENZIONE: Tali dati non devono essere utilizzati per controllare direttamente un'uscita SIL 3/PLe.
4	I tag di sicurezza dell'ambito del controllore possono essere letti direttamente dalla logica standard.
5	I tag di sicurezza possono essere letti o scritti dalla logica di sicurezza.
6	I tag di sicurezza possono essere scambiati tra i controllori di sicurezza su reti Ethernet o ControlNet, ivi compresi i controllori GuardLogix 1756 e 1768.
7	I dati di tag di sicurezza, dell'ambito del programma o del controllore, possono essere letti da dispositivi esterni, quali dispositivi di interfaccia operatore, personal computer o altri controllori standard.
	IMPORTANTI Dopo essere stati letti, tali dati sono considerati di tipo standard e non SIL 3/PLe.

Scelta dell'hardware del sistema

Il sistema GuardLogix supporta le applicazioni di sicurezza SIL 3 e PLe. Il controllore GuardLogix è costituito da un controllore primario e da un coprocessore di sicurezza che funzionano insieme in un'architettura 1oo2. La Tabella 4 elenca i numeri di catalogo dei controllori primari e dei coprocessori di sicurezza.

Il coprocessore di sicurezza deve essere installato nello slot immediatamente a destra del controllore primario. Le versioni principale e secondaria del firmware del controllore primario e del coprocessore di sicurezza devono corrispondere esattamente affinché venga stabilita la partnership di controllo necessaria per le applicazioni di sicurezza.

Tabella 4 - Numeri di catalogo dei controllori primari e dei corrispondenti coprocessori di sicurezza

Controllore primario	Coprocessore di sicurezza
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

Controllore primario

Il controllore primario è il processore che esegue sia le funzioni standard sia quelle di sicurezza e che comunica con il coprocessore di sicurezza per le funzioni di sicurezza del sistema di controllo GuardLogix. Di seguito è riportato un elenco di funzioni standard:

- Controllo I/O
- Logica
- Temporizzazione
- Conteggio
- Generazione rapporti
- Comunicazione
- Calcoli aritmetici
- Manipolazione file dati

Il controllore primario è costituito da un processore centrale, dall'interfaccia I/O e dalla memoria.

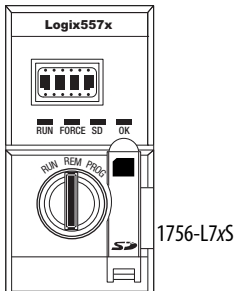
Tabella 5 - Capacità memoria

N. catalogo	Memoria utente (capacità RAM)	
	Task e componenti standard	Task e componenti di sicurezza
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S,1756-L73SXT	8 MB	4 MB

Un selettore a chiave a tre posizioni situato nella parte anteriore del controllore primario controlla le modalità di funzionamento del controllore. Sono disponibili le seguenti modalità:

- RUN (esecuzione)
- PROG (programmazione)
- REM (remota): questa modalità abilitata dal software può essere Programmazione, Esecuzione o Test

Figura 2 – Posizioni del selettore a chiave



Coprocessore di sicurezza

Il coprocessore di sicurezza è quello che fornisce un secondo canale isolato (ridondanza) per le funzioni di sicurezza del sistema.

Il coprocessore di sicurezza non dispone di un selettore a chiave o di una porta di comunicazione. La configurazione ed il funzionamento sono controllati dal controllore primario.

Chassis

Lo chassis ControlLogix fornisce connessioni fisiche tra i moduli e il controllore GuardLogix.

Alimentatore

Gli alimentatori ControlLogix elencati a pagina 25 possono essere utilizzati in applicazioni SIL 3. Per il funzionamento SIL 3 degli alimentatori non sono necessarie configurazioni o collegamenti aggiuntivi.

Scelta dei dispositivi I/O di sicurezza

I dispositivi di sicurezza di ingresso e uscita, come sensori ed attuatori, possono essere collegati all'I/O di sicurezza su reti DeviceNet o EtherNet/IP. Questa connessione consente il controllo dei dispositivi di uscita tramite il sistema controllore GuardLogix attraverso comunicazioni DeviceNet o EtherNet/IP.

Per informazioni aggiornate sui numeri di catalogo, le serie certificate e le versioni firmware disponibili per gli I/O di sicurezza, consultare i certificati di sicurezza all'indirizzo http://www.rockwellautomation.com/rockwellautomation/certification/safety.page.

Scelta delle reti di comunicazione

Il controllore GuardLogix supporta funzioni di comunicazione che consentono di:

- Distribuire e controllare l'I/O di sicurezza su reti DeviceNet o EtherNet/IP
- Distribuire e controllare i moduli I/O di sicurezza remoti su reti DeviceNet, EtherNet/IP o ControlNet
- Produrre e consumare i dati dei tag di sicurezza tra i controllori GuardLogix 1756 e 1768 attraverso una rete Ethernet/IP o ControlNet, oppure all'interno dello stesso chassis ControlLogix
- Distribuire e controllare i moduli I/O standard su reti EtherNet, ControlNet o DeviceNet

Utilizzare questi moduli di comunicazione per fornire un'interfaccia tra i controllori GuardLogix e i dispositivi di rete.

Tabella 6 - Moduli di comunicazione

Come interfaccia tra	Utilizzare il modulo	Vedere queste istruzioni per l'installazione
Il controllore GuardLogix e i dispositivi DeviceNet	1756-DNB	DNET-IN001
Il controllore GuardLogix e i dispositivi EtherNet/IP	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR 1756-EN2TXT 1756-EN2TRXT	ENET-IN002
Controllori sulla rete ControlNet	1756-CN2 1756-CN2R 1756-CN2RXT	CNET-IN005

Il controllore GuardLogix può collegarsi all'applicazione Logix Designer attraverso una porta USB, un modulo EtherNet o un modulo ControlNet.

Per ulteriori informazioni sui moduli di comunicazione di rete, vedere Per ulteriori informazioni a pagina 11.

Requisiti di programmazione

Per identificare lo strumento di programmazione e le versioni da utilizzare con i controllori GuardLogix 5570, vedere la Tabella 7.

Tabella 7 - Versioni software

N. catalogo	Ambiente Studio 5000	Versione software RSLogix 5000(1)	Versione software RSLinx® Classic
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	21 o successiva	20 o successiva	2.59 o successiva

(1) Per informazioni su come utilizzare un controllore GuardLogix con il software RSLogix 5000, consultare il Manuale dell'utente Controllori GuardLogix, pubblicazione 1756-UM020I-IT-P e GuardLogix Controller Systems Safety Reference Manual, pubblicazione 1756-RM093.

Le routine di sicurezza includono le istruzioni di sicurezza, che sono un sottoinsieme del set di istruzioni della logica ladder standard, e le istruzioni per le applicazioni di sicurezza. I programmi schedulati nell'ambito del task di sicurezza supportano solo la logica ladder.

Tabella 8 - Funzioni supportate

	Applicazione Logix Designer di Studio 5000	
	Versione 24 e successive	
Funzione	**Task di sicurezza**	**Task standard**
Istruzioni Add-on	X	X
Allarmi ed eventi		
Registro controllore	X	
Controllo dell'accesso ai dati		
Routine fasi apparecchiatura		
Task evento		
Firmware Supervisor	X	
Diagrammi a blocchi funzione (FBD)		
Controllo assi		
Logica ladder	X	
Cambio di lingua		
Scheda di memoria		
Traduzione degli indirizzi di rete (NAT)		
Importazione ed esportazione online di componenti dei programmi		
Connessioni di sicurezza e standard	X	
Routine in diagramma funzionale sequenziale (SFC)		
Testo strutturato		
Connessioni unicast per tag di sicurezza prodotti e consumati	X	
Connessioni unicast per dispositivi I/O di sicurezza su reti EtherNet/IP		

Per informazioni su come utilizzare queste funzioni, consultare Logix5000 Controllers Common Procedures Programming Manual, pubblicazione 1756-PM001, le pubblicazioni elencate in Per ulteriori informazioni a pagina 11 e la guida online.

Note:

Installazione del controllore

Argomento	Pagina
Precauzioni	21
Verificare di avere tutti i componenti	24
Installazione di un alimentatore e di uno chassis	25
Installazione del controllore nello chassis	25
Inserimento o rimozione di una scheda di memoria	26
Collegamenti di comunicazione	29
Aggiornamento del controllore	31
Scelta della modalità operativa del controllore	33
Disinstallazione del modulo di alimentazione (ESM)	34
Installazione di un modulo di alimentazione (ESM)	36

Precauzioni

Leggere e rispettare le seguenti precauzioni d'uso.

Informazioni ambientali e sulla custodia

ATTENZIONE: Questa apparecchiatura è destinata all'uso in ambienti industriali con Grado di Inquinamento 2, in applicazioni con sovratensione di categoria II, (come definito nello standard IEC 60664-1) ad altitudine fino a 2.000 metri senza declassamento.

Questa apparecchiatura non è destinata all'uso in ambienti residenziali e, in tali ambienti, può non garantire un'adeguata protezione ai servizi di comunicazione radio.

L'apparecchiatura viene fornita come apparecchiatura di tipo aperto. L'apparecchiatura deve essere montata all'interno di una custodia adatta alle specifiche condizioni ambientali di utilizzo e progettata specificatamente per evitare lesioni al personale derivanti dall'accesso a parti in tensione. La custodia deve avere opportune caratteristiche ignifughe, al fine di prevenire o di ridurre al minimo la propagazione delle fiamme, deve essere conforme ad una classe di autoestinguenza 5VA o essere approvata per l'applicazione se non metallica. Deve essere possibile accedere all'interno della custodia solo mediante uno strumento. Le successive sezioni di questa pubblicazione possono contenere ulteriori informazioni circa specifici tipi di custodie richieste per la conformità alle certificazioni di sicurezza di alcuni prodotti.

Oltre alla presente, per ulteriori informazioni, consultare le seguenti pubblicazioni:

- Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1, per ulteriori requisiti di installazione
- Per ulteriori informazioni sui gradi di protezione forniti dai diversi tipi di custodia, vedere gli standard NEMA 250 ed IEC 60529

Sistemi elettronici programmabili (PES, Programmable Electronic Systems)

ATTENZIONE: Il personale responsabile dell'applicazione dei sistemi elettronici programmabili (PES) di sicurezza deve conoscere i requisiti di sicurezza nell'applicazione del sistema e deve aver ricevuto l'adeguata formazione sull'utilizzo del sistema.

Rimozione e inserimento sotto tensione (RIUP, Removal and Insertion Under Power)

AVVERTENZA. Quando si inserisce o si rimuove il modulo con il backplane in tensione, può verificarsi un arco elettrico. Ciò potrebbe provocare un'esplosione in caso di installazioni in aree pericolose.

Prima di procedere, assicurarsi di aver tolto l'alimentazione o che l'area non sia pericolosa. Ripetuti archi elettrici causano l'eccessiva usura dei contatti sia sul modulo che sul relativo connettore di accoppiamento. I contatti usurati possono generare una resistenza elettrica che può incidere negativamente sul funzionamento del modulo.

Approvazione nordamericana per l'uso in aree pericolose

The following information applies when operating this equipment in hazardous locations.	**Le seguenti informazioni si riferiscono al caso in cui questa apparecchiatura operi in un'area pericolosa.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	I prodotti contrassegnati con "CL I, DIV 2, GP A, B, C, D" sono adatti all'utilizzo solo in aree pericolose di Classe I Divisione 2 Gruppi A, B, C, D, o in aree non pericolose. Ogni prodotto è dotato di una targhetta dati indicante il codice temperatura dell'area pericolosa. Quando si integrano prodotti diversi per formare un sistema, utilizzare il codice temperatura più conservativo (valore minimo "T") per determinare il codice temperatura generale del sistema. L'uso di apparecchiature diverse all'interno del sistema è soggetto ad ispezione da parte delle autorità locali competenti al momento dell'installazione.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**AVVERTENZA.** RISCHIO DI ESPLOSIONI • Non scollegare l'apparecchio prima di aver rimosso l'alimentazione, a meno che non si sia certi che l'area non è pericolosa. • Non scollegare i collegamenti di questa apparecchiatura senza aver prima interrotto l'alimentazione oppure senza essere certi di operare in un ambiente non pericoloso. Fissare tutti i collegamenti esterni a questa apparecchiatura con viti, dispositivi di aggancio scorrevoli, connettori filettati o altri mezzi forniti insieme al prodotto. • La sostituzione dei componenti può compromettere l'idoneità per gli ambienti della classe I, Divisione 2. • Se il prodotto contiene batterie, queste vanno sostituite esclusivamente in aree non pericolose.

Approvazione europea per aree pericolose

L'apposizione della marcatura Ex sul prodotto certifica quanto segue.

Questa apparecchiatura è destinata all'uso in atmosfere potenzialmente esplosive, come definite dalla Direttiva 94/9/CE dell'Unione Europea, ed è risultata conforme ai requisiti essenziali di sicurezza e salute riguardanti la progettazione e la costruzione di apparecchiature di Categoria 3 destinate all'uso in atmosfere potenzialmente esplosive di Zona 2, riportate nell'Allegato II di questa direttiva.

La conformità ai requisiti essenziali di sicurezza e salute è assicurata dalla conformità alle norme EN 60079-15 ed EN 60079-0.

ATTENZIONE: Questa apparecchiatura non è resistente alla luce del sole o ad altre fonti di radiazione UV.

AVVERTENZA. Per il montaggio e l'uso dell'apparecchiatura, osservare le seguenti regole generali:

- Montare l'apparecchiatura in una custodia certificata ATEX con grado di protezione minimo IP54 (come definito in IEC60529) e utilizzarla in un ambiente con grado di inquinamento non superiore a 2 (come definito in IEC 60664-1) in caso di uso in ambienti di Zona 2. Il portello o il coperchio della custodia deve essere rimovibile con un attrezzo.
- L'apparecchiatura deve essere utilizzata entro i valori nominali specificati da Rockwell Automation.
- L'apparecchiatura deve essere utilizzata solo con backplane certificati ATEX di Rockwell Automation.
- Non scollegare l'apparecchiatura senza aver prima interrotto l'alimentazione oppure senza essere certi di operare in un ambiente non pericoloso.

In caso di utilizzo in ambienti di Zona 2, adottare le contromisure necessarie a prevenire il superamento della tensione nominale dovuto a transitori elettrici superiori al 140% della tensione nominale.

Fissare tutti i collegamenti esterni a questa apparecchiatura con viti, dispositivi di aggancio scorrevoli, connettori filettati o altri mezzi forniti insieme all'apparecchiatura.

Prevenzione delle scariche elettrostatiche

ATTENZIONE: Questa apparecchiatura è sensibile alle scariche elettrostatiche. Queste possono provocare danni interni ed influenzarne il funzionamento. Quando si maneggia l'apparecchiatura, osservare le seguenti regole generali:

- Scaricare l'elettricità statica toccando un oggetto messo a terra.
- Indossare un braccialetto di messa a terra omologato.
- Non toccare i connettori o i pin delle schede.
- Non toccare i componenti dei circuiti interni dell'apparecchiatura.
- Se disponibile, usare una stazione di lavoro antistatica.
- Quando non viene utilizzata, conservare l'apparecchiatura in un imballaggio antistatico.

Verificare di avere tutti i componenti

Prima di iniziare, controllare di disporre di tutti i componenti necessari.

IMPORTANTE Per ottenere il livello SIL 3/PLe, è necessario usare un controllore primario **e** un coprocessore di sicurezza.

Con il controllore primario e il coprocessore di sicurezza sono inclusi i seguenti componenti.

N. catalogo	Descrizione	Fornito con
1756-L71S 1756-L72S 1756-L73S	Controllore primario	• 1756-ESMCAP – Modulo di alimentazione (ESM) con condensatore • 1784-SD1 - Scheda di memoria SD, 1 GB • 1747-KY – Chiave
1756-L7SP	Coprocessore di sicurezza	• 1756-SPESMNSE – Modulo di alimentazione (ESM)
1756-L73SXT	Controllore primario per temperature estreme	• 1756-ESMCAPXT – Modulo di alimentazione (ESM) con condensatore • 1747-KY – Chiave
1756-L7SPXT	Coprocessore di sicurezza per temperature estreme	• 1756-SPESMNSEXT – Modulo di alimentazione (ESM) con condensatore

È possibile utilizzare le seguenti apparecchiature opzionali.

Se l'applicazione richiede	Usare quanto segue
Memoria non volatile	1784-SD1 (1 GB) oppure 1784-SD2 (2 GB)
Che il modulo ESM installato scarichi l'energia residua a 200 µJ o meno, prima di rimuoverlo o inserirlo nell'applicazione.(1)	1756-ESMNSE per il controllore primario 1756-SPESMNSE per il coprocessore di sicurezza(2) Questo modulo ESM non prevede l'alimentazione di backup dell'orologio interno (WallClockTime). Questo modulo ESM, inoltre, può essere utilizzato soltanto con un'unità 1756-L73S (8 MB) o con un controllore di memoria inferiore.
Modulo ESM che protegge il controllore impedendo l'uso della porta USB e della scheda SD(1)	1756-ESMNRM per il controllore primario 1756-SPESMNRM per il coprocessore di sicurezza(3) Questo modulo ESM garantisce all'applicazione un grado di sicurezza superiore.

(1) Per informazioni sul tempo di autonomia dei moduli ESM, vedere la sezione Valutazione dell'alimentazione dell'orologio interno (WallClockTime) da parte del modulo ESM a pagina 118.

(2) Con i controllori primari e i coprocessori di sicurezza per temperature estreme, usare 1756-ESMNSEXT e 1756-SPESMNSEXT rispettivamente.

(3) Con i controllori primari d i coprocessori di sicurezza per temperature estreme, usare 1756-ESMNRMXT e 1756-SPESMNRMXT rispettivamente

Installazione di un alimentatore e di uno chassis

Prima di installare un controllore, è necessario installare uno chassis e un alimentatore.

1. Installare uno chassis ControlLogix attenendosi alle corrispondenti istruzioni per l'installazione.

N. catalogo	Slot disponibili	Serie	Fare riferimento alle istruzioni per l'installazione
1756-A4	4	B	1756-IN005
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

I controllori per temperature estreme (XT) richiedono uno chassis XT.

2. Installare un alimentatore ControlLogix attenendosi alle corrispondenti istruzioni per l'installazione.

N. catalogo	Descrizione	Serie	Fare riferimento alle istruzioni per l'installazione
1756-PA72	Alimentatore, CA	C	1756-IN005
1756-PB72	Alimentatore, CC		
1756-PA75	Alimentatore, CA	B	
1756-PB75	Alimentatore, CC		
1756-PAXT	Alimentatore XT, CA	B	
1756-PBXT	Alimentatore XT, CC		

I controllori per temperature estreme (XT) richiedono un alimentatore XT.

Installazione del controllore nello chassis

I controllori possono essere installati o rimossi mentre lo chassis è in tensione con il sistema funzionante.

AVVERTENZA. Se si inserisce o si rimuove il modulo con l'alimentazione backplane inserita, potrebbe verificarsi un arco elettrico. Ciò potrebbe provocare un'esplosione in caso di installazioni in aree pericolose.

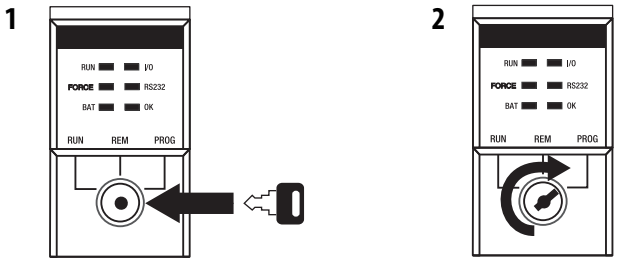
Prima di procedere, assicurarsi di aver tolto l'alimentazione o che l'area non sia pericolosa. Il ripetuto verificarsi di archi elettrici provoca l'eccessiva usura dei contatti, sia del modulo sia del connettore corrispondente. I contatti usurati possono generare una resistenza elettrica che può incidere negativamente sul funzionamento del modulo.

IMPORTANTE Il modulo ESM inizia a caricare in occasione di una delle seguenti operazioni:

- Installazione di controllore e modulo ESM in uno chassis in tensione.
- Messa in tensione di uno chassis in cui è presente un controllore con modulo ESM installato.
- Installazione di un modulo ESM in un controllore in tensione.

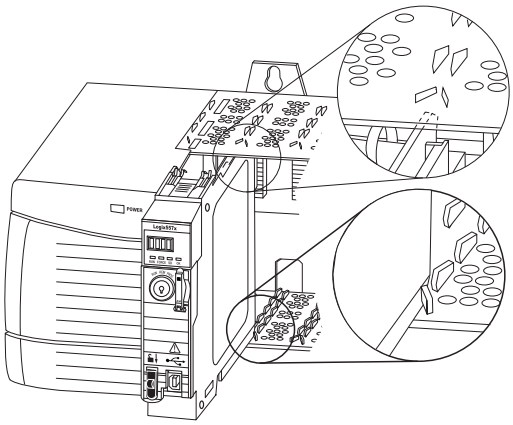
Dopo la messa in tensione, il modulo ESM si carica per un periodo massimo di due minuti, come indicato dal messaggio CHRG o ESM Charging sul display di stato.

1. Inserire la chiave nel controllore primario.
2. Girare la chiave in posizione PROG.



Il coprocessore di sicurezza non è dotato di selettore a chiave.

3. Allineare il circuito con le guide superiore e inferiore nello chassis.



4. Far scorrere il controllore nello chassis.

Il controllore è perfettamente installato quando risulta allineato con l'alimentatore o gli altri moduli installati e quando i dispositivi di blocco superiore ed inferiore sono agganciati.

IMPORTANTE Il coprocessore di sicurezza deve essere installato nello slot immediatamente a destra del controllore primario. Per installare il coprocessore di sicurezza, seguire le stesse procedure di cui ai punti 3 e 4 sopra.

Dopo aver inserito il controllore nello chassis, vedere Capitolo 9 per informazioni sulla lettura degli indicatori di stato del controllore primario e del coprocessore di sicurezza.

Inserimento o rimozione di una scheda di memoria

AVVERTENZA. Se si inserisce o si estrae la scheda di memoria con l'alimentazione inserita, potrebbe verificarsi un arco elettrico. Ciò potrebbe provocare un'esplosione in caso di installazioni in aree pericolose. Prima di procedere, assicurarsi di aver tolto l'alimentazione o che l'area non sia pericolosa.

ATTENZIONE: Se **non** si è sicuri del contenuto della scheda di memoria, **prima** di installarla, portare il selettore a chiave del controllore in posizione PROG. A seconda del contenuto della scheda, un ciclo di spegnimento/riaccensione o un errore potrebbero causare il caricamento di un progetto o di un sistema operativo differente nel controllore.

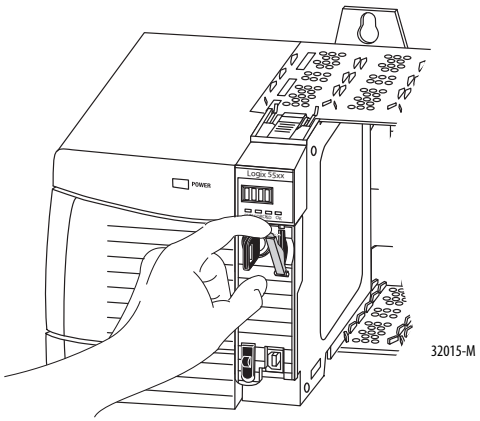
Il controllore viene fornito con una scheda SD preinstallata, che è consigliabile lasciare installata.

Rimozione della scheda SD

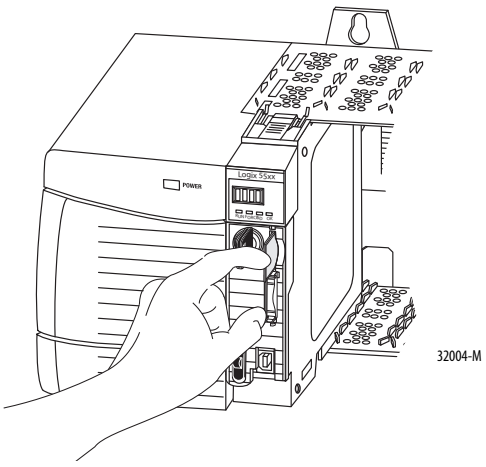
Per rimuovere la scheda SD procedere come segue.

IMPORTANTE Verificare che l'indicatore di stato della scheda SD sia spento e che la scheda non sia in uso, prima di rimuoverla.

1. Portare il selettore a chiave sulla posizione PROG.
2. Aprire il portellino per accedere alla scheda SD.



3. Premere e rilasciare la scheda SD per estrarla.

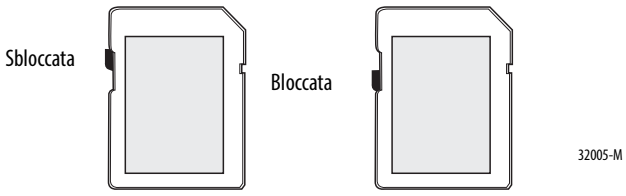


4. Rimuovere la scheda SD e chiudere il portellino.

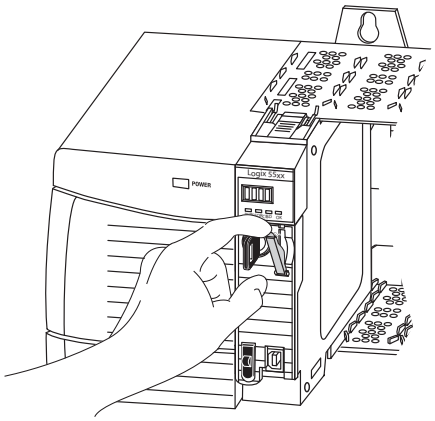
Installazione della scheda SD

Per installare la scheda SD, procedere come segue.

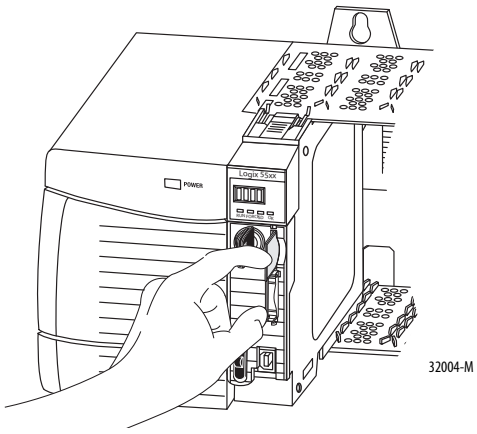
1. Verificare che la scheda SD sia bloccata o sbloccata, a seconda delle preferenze.



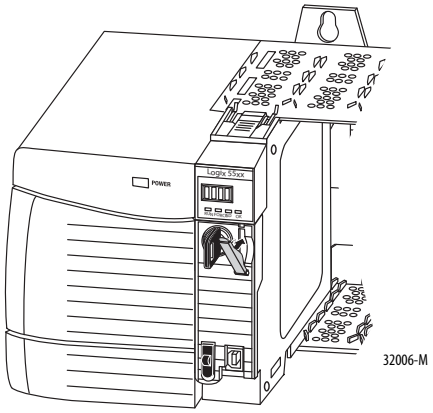
2. Aprire il portellino per la scheda SD.



3. Inserire la scheda SD nell'apposito slot.
4. Premere la scheda delicatamente fino a quando scatta in posizione.



5. Chiudere il portellino della scheda SD.



Collegamenti di comunicazione

Il controllore ha una porta USB con una presa di Tipo B. Il collegamento è compatibile con lo standard USB 2.0- e funziona a 12 Mbps.

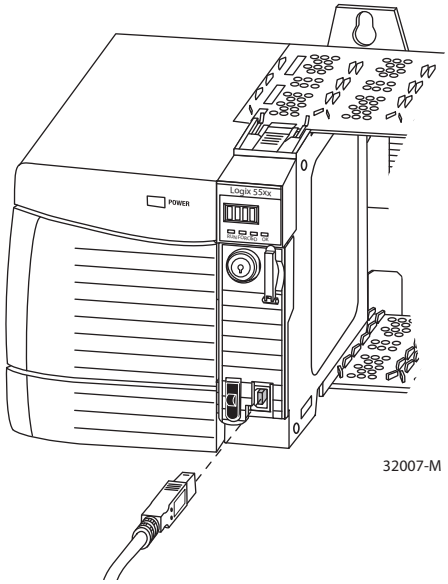
Per usare la porta USB del controllore, è necessario avere installato sul computer il software RSLinx, versione 2.59 o successiva. Per collegare il computer alla porta USB, usare un cavo USB. Con questo collegamento, è possibile aggiornare il firmware e scaricare i programmi nel controllore direttamente dalla workstation.

ATTENZIONE: La porta USB può essere utilizzata per finalità di programmazione locali e temporanee. Non utilizzare la porta USB per collegamenti permanenti.

Il cavo USB non deve superare i 3,0 m e non deve contenere hub.

AVVERTENZA. Non utilizzare la porta USB in aree pericolose.

Figura 3 – Porta USB



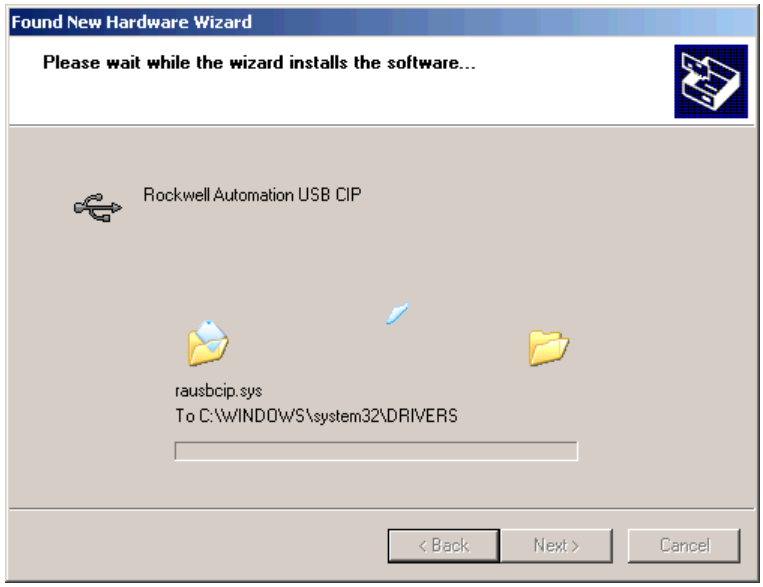
Per configurare il software RSLinx per l'utilizzo di una porta USB, è necessario configurare prima un driver USB. Per configurare un driver USB, procedere come segue.

1. Collegare controllore e computer con un cavo USB.
2. Nella finestra di dialogo Found New Hardware Wizard, fare clic su una delle opzioni di connessione a Windows Update e fare clic su Next.

SUGGERIMENTO Se il software per il driver USB non è disponibile e l'installazione viene annullata, verificare di aver installato il software RSLinx Classic, versione 2.59 o successiva.

3. Fare clic su Install the software automatically (raccomandato) e fare clic su Next.

   Il software è installato.

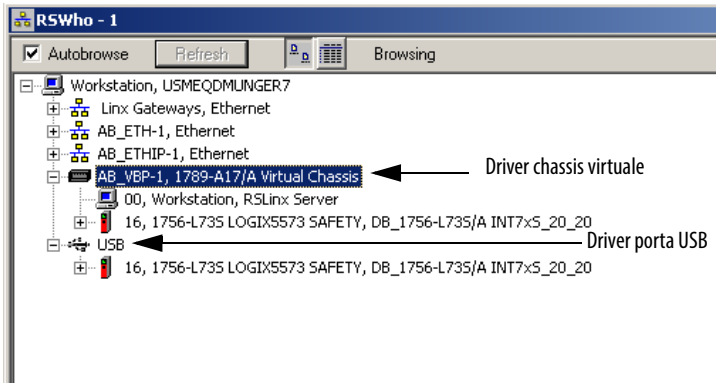


4. Fare clic su Finish per configurare il driver USB.

5. Per selezionare il controllore nel software RSLinx, fare clic su RSWho

   .

   Nell'organizer di RSLinx Workstation, il controllore viene visualizzato in due driver differenti, uno chassis virtuale e la porta USB. Per selezionare il controllore, è possibile usare entrambi i driver.



Aggiornamento del controllore

I controllori vengono forniti senza firmware. Il firmware del controllore è integrato nell'ambiente Studio 5000. Inoltre, il firmware del controllore può essere scaricato dal sito Web dedicato all'assistenza tecnica di Rockwell Automation, all'indirizzo: http://www.rockwellautomation.com/support/.

È possibile aggiornare il firmware usando il software ControlFLASH™ o la funzione AutoFlash dell'applicazione Logix Designer.

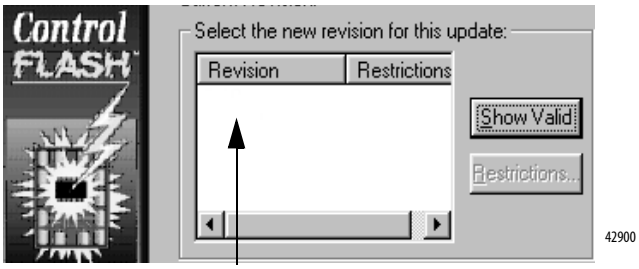
Utilizzo del software ControlFLASH per l'aggiornamento del firmware

Il coprocessore di sicurezza si aggiorna automaticamente quando il controllore primario viene aggiornato.

IMPORTANTE	Se la scheda SD è bloccata e l'opzione Load Image del progetto memorizzato è impostata su On Power Up, il firmware del controllore non viene aggiornato dopo queste operazioni. Vengono invece caricati eventuali progetti e il firmware memorizzati precedentemente.

1. Verificare che la connessione di rete sia effettiva e corretta e che, nel software RSLinx, sia configurato il driver di rete.
2. Avviare il software ControlFLASH.
3. Selezionare Next.
4. Selezionare il numero di catalogo del controllore e fare clic su Next.
5. Espandere la rete fino a visualizzare il controllore.

6. Selezionare il controllore e fare clic su Next.



7. Selezionare il livello di versione dell'aggiornamento del controllore e fare clic su Next.
8. Per avviare l'aggiornamento del controllore, fare clic su Finish e poi su Yes.

   Al completamento dell'aggiornamento, viene visualizzato il messaggio "Update complete".

IMPORTANTE	Attendere il completamento dell'aggiornamento del firmware prima di spegnere e riaccendere o interrompere in altro modo l'aggiornamento.

SUGGERIMENTO	Se l'aggiornamento ControlFLASH del controllore viene interrotto, il controllore torna al firmware di avvio, ovvero alla versione firmware 1.*xxx*.

9. Fare clic su OK.
10. Chiudere il software ControlFLASH.

Utilizzo di AutoFlash per l'aggiornamento del firmware

Per aggiornare il firmware del controllore con la funzione AutoFlash, procedere come segue.

1. Verificare che la connessione di rete sia effettiva e corretta e che, nel software RSLinx, sia configurato il driver di rete.
2. Usare l'applicazione Logix Designer per creare un progetto controllore con la versione necessaria.

3. Fare clic su RSWho per specificare il percorso del controllore.

4. Selezionare il controllore e fare clic su Update Firmware.
5. Selezionare la versione del firmware desiderata.

6. Fare clic su Update.
7. Fare clic su Yes.

Lasciar completare l'aggiornamento firmware senza interruzioni. Quando l'aggiornamento del firmware è terminato, si apre la finestra di dialogo Who Active. Nell'applicazione Logix Designer è possibile completare altre attività.

Scelta della modalità operativa del controllore

Fare riferimento a questa tabella per determinare la modalità operativa del controllore.

Tabella 9 - Modalità operative del controllore

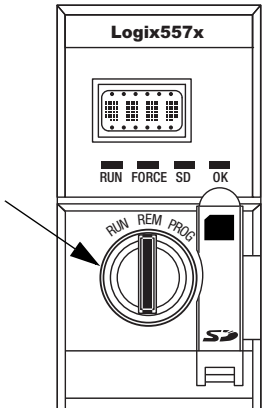
Se si desidera	Selezionare una di queste modalità				
	Esecuzione	Remota			Programmazione
		Esecuzione	Test	Programmazione	
Commutare le uscite sullo stato comandato dalla logica del progetto	X	X			
Commutare le uscite sullo stato configurato per la modalità Programmazione			X	X	X
Eseguire (scandire) task	X	X	X		
Cambiare la modalità del controllore attraverso il software		X	X	X	
Scaricare un progetto		X	X	X	X
Schedulare una rete ControlNet				X	X
Modificare il progetto online		X	X	X	X
Inviare messaggi	X	X	X		
Inviare e ricevere dati in risposta ad un messaggio da un altro controllore	X	X	X	X	X
Produrre e consumare tag	X	X	X	X	X

Uso del selettore a chiave per cambiare la modalità operativa

Il selettore a chiave situato nella parte frontale del controllore può essere utilizzato per portare il controllore in una delle seguenti modalità:

- Programmazione (PROG)
- Remota (REM)
- Esecuzione (RUN)

Figura 4 – Selettore a chiave del controllore



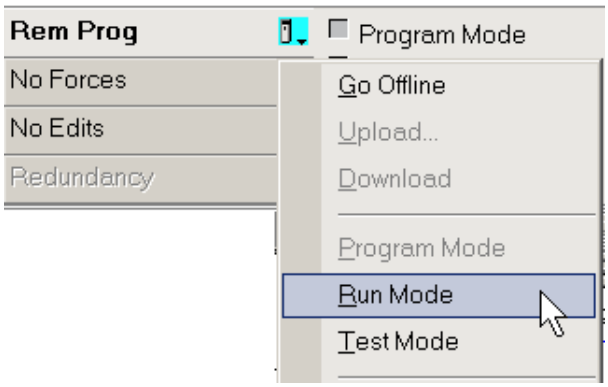
Utilizzo dell'applicazione Logix Designer per cambiare la modalità operativa

In base alla modalità specificata per il controllore con il selettore a chiave, è possibile cambiare la modalità operativa del controllore attraverso l'applicazione Logix Designer.

Con il controllore online e il selettore a chiave impostato su Remota (REM, posizione centrale), è possibile usare il menu Controller Status nell'angolo superiore sinistro della finestra dell'applicazione Logix Designer per specificare le seguenti modalità operative:

- Programmazione remota
- Esecuzione remota
- Test remoto

Figura 5 – Modalità operativa tramite l'applicazione Logix Designer



SUGGERIMENTO In questo esempio, il selettore a chiave del controllore è impostato su Modalità Remota. Se il selettore a chiave del controllore è impostato su Modalità Esecuzione o Modalità Programmazione, le opzioni del menu cambiano.

Disinstallazione del modulo di alimentazione (ESM)

I controllori vengono forniti con un modulo ESM installato.

Controllore	N. catalogo ESM installato
1756-L7xS – controllore	1756-ESMCAP
1756-L7xSXT – controllore per temperature estreme	1756-ESMCAPXT
1756-L7SP – coprocessore di sicurezza	1756-SPESMNSE
1756-L7SPXT – coprocessore di sicurezza per temperature estreme	1756-SPESMNSEXT

Prima di rimuovere il modulo ESM, considerare quanto segue:

- Anche quando il controllore non è più in tensione, per interruzione dell'alimentazione allo chassis o perché rimosso da uno chassis alimentato, non rimuovere immediatamente il modulo ESM.

  Prima di rimuovere il modulo ESM, attendere che l'indicatore di stato OK del controllore passi da verde a rosso fisso e poi si spenga.

- Usare il modulo 1756-ESMNSE se l'applicazione richiede che il modulo ESM installato riduca l'energia residua a 40 µJoule o meno prima di installarlo o rimuoverlo dall'applicazione.
- Una volta installato, il modulo 1756-ESMNRM non può essere rimosso dal controllore.

IMPORTANTE Prima di rimuovere un modulo ESM, apportare al programma le regolazioni necessarie in considerazione delle potenziali modifiche all'attributo WallClockTime.

Per rimuovere un modulo 1756-ESMCAP(XT), 1756-ESMNSE(XT) o 1756-SPESMNSE(XT), procedere come segue.

AVVERTENZA. Se l'applicazione richiede che il modulo ESM riduca la sua energia residua a 40 µJoule o meno prima di inserirlo o rimuoverlo dall'applicazione, usare il modulo 1756-ESMNSE(XT) per il controllore primario e il modulo 1756-SPESMNSE(XT) per il coprocessore di sicurezza. In tal caso, prima di rimuovere il modulo ESM, procedere come segue.

a. Interrompere l'alimentazione dello chassis.
   Dopo l'interruzione dell'alimentazione allo chassis, l'indicatore di stato OK del controllore passa da verde a rosso fisso e poi si spegne.
b. Attendere **almeno 20 minuti** perché l'energia residua scenda a 40 µJ o meno prima di rimuovere il modulo ESM.
   Non è prevista una segnalazione visiva allo scadere dei 20 minuti. **È necessario tenerne conto personalmente**.

AVVERTENZA. Se si inserisce o si rimuove il modulo di alimentazione con l'alimentazione backplane inserita, potrebbe verificarsi un arco elettrico. Ciò potrebbe provocare un'esplosione in caso di installazioni in aree pericolose.

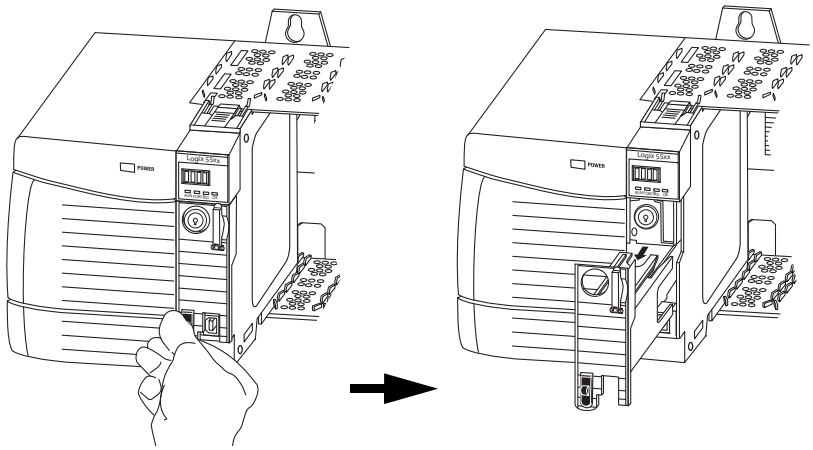
Prima di procedere, assicurarsi di aver tolto l'alimentazione o che l'area non sia pericolosa. Il ripetuto verificarsi di archi elettrici provoca l'eccessiva usura dei contatti, sia del modulo sia del connettore corrispondente.

1. Estrarre la chiave dal selettore a chiave.

IMPORTANTE Il passo successivo dipende da quale delle seguenti condizioni è valida per la propria applicazione:

- Se il modulo ESM viene rimosso da un controllore in tensione, andare al passaggio 2.
- Se il modulo ESM viene rimosso da un controllore non in tensione, a causa dell'interruzione dell'alimentazione dello chassis o della rimozione del controllore da uno chassis alimentato, **non rimuovere** immediatamente il modulo ESM.
  Prima di rimuovere il modulo ESM, attendere che l'indicatore di stato OK del controllore passi da verde a rosso fisso e poi si spenga.
  Quando l'indicatore di stato OK si spegne, andare al passaggio 2.

2. Premere il pulsante di sblocco nero con il pollice ed estrarre il modulo ESM dal controllore.



Installazione di un modulo di alimentazione (ESM)

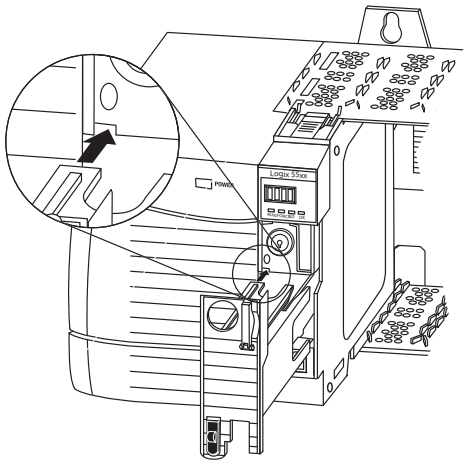
La Tabella 10 elenca i moduli ESM e i controllori GuardLogix compatibili.

Tabella 10 - Moduli di alimentazione compatibili

N. catalogo	ESM compatibili
1756-L7*x*S	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7*x*SXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Per installare un modulo ESM, procedere come segue. Attenersi alla stessa procedura per il coprocessore di sicurezza.

1. Allineare gli slot ad incastro del modulo ESM e del controllore.



2. Far scorrere il modulo ESM nello chassis fino a quando scatta in posizione.

ATTENZIONE: Per evitare di danneggiare il prodotto quando si inserisce il modulo ESM, allinearlo nella guida e spingerlo delicatamente fino a quando scatta in posizione.

Dopo l'installazione, il modulo ESM inizia a caricarsi. Lo stato di carica è indicato da uno dei seguenti messaggi di stato:

- ESM Charging
- CHRG

Dopo aver installato il modulo ESM, possono trascorrere fino a 15 secondi prima di visualizzare i messaggi sullo stato di carica.

IMPORTANTE	Prima di interrompere l'alimentazione del controllore, lasciar completare l'operazione di carica del modulo ESM. Per verificare che il modulo ESM sia completamente carico, controllare che sul display di stato non compaiano più i messaggi "CHRG" o "ESM Charging".
SUGGERIMENTO	Dopo aver installato un modulo ESM, controllare gli attributi dell'oggetto WallClockTime per verificare che l'ora del controllore sia corretta.

Note:

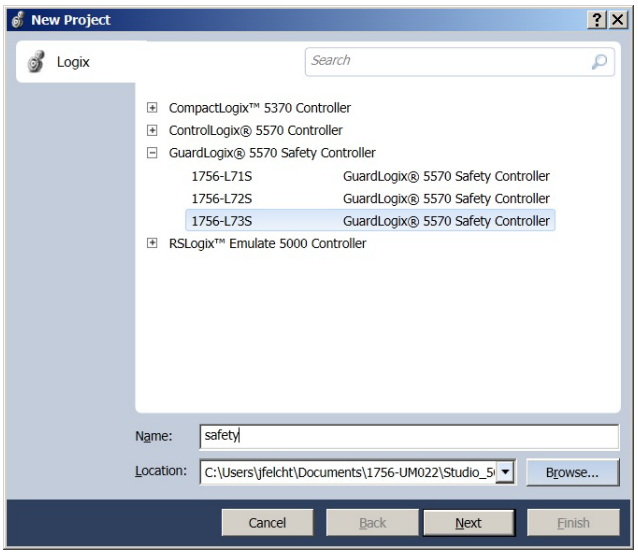
Configurazione del controllore

Argomento	Pagina
Creazione di un progetto del controllore	39
Codifica elettronica	42
Impostazione delle -password per il blocco/sblocco di sicurezza	42
Protezione della firma del task di sicurezza in modalità Esecuzione	43
Gestione della sostituzione dei moduli I/O	44
Abilitazione della sincronizzazione temporale	45
Configurazione di un controllore di sicurezza peer	45

Creazione di un progetto del controllore

Per configurare e programmare un controllore, si utilizza l'applicazione Logix Designer per creare e gestire un progetto per il controllore.

1. Per creare un progetto, fare clic sul pulsante New sulla barra degli strumenti principale.
2. Per espandere l'elenco dei possibili controllori, fare doppio clic sul controllore di sicurezza GuardLogix 5570.
3. Selezionare un controllore GuardLogix:
   - 1756-L71S Controllore di sicurezza GuardLogix 5570
   - 1756-L72S Controllore di sicurezza GuardLogix 5570
   - 1756-L73S Controllore di sicurezza GuardLogix 5570

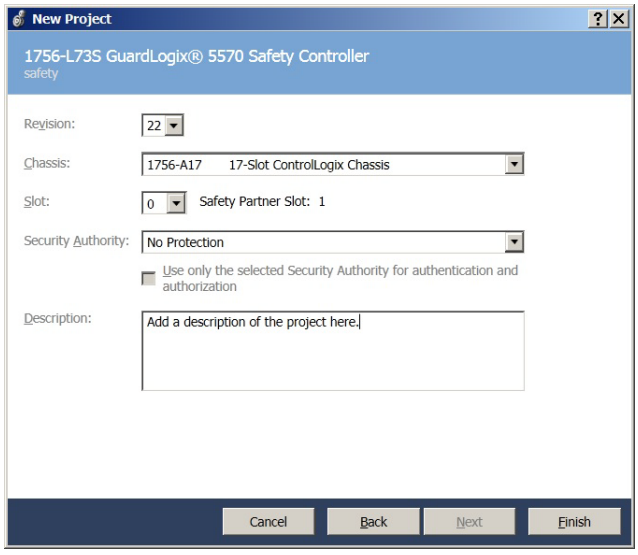


4. Nel campo Name, immettere il nome del progetto.
5. Per specificare in quale cartella archiviare il progetto del controllore di sicurezza, fare clic su Browse.
6. Fare clic su Next.

7. Nel menu a discesa Revision, selezionare il numero di versione principale del firmware del controllore.
8. Nel menu a discesa Chassis, selezionare la dimensione dello chassis.
9. Nel menu a discesa Slot, selezionare lo slot per il coprocessore di sicurezza.

   Nella finestra di dialogo New Project viene visualizzata la posizione dello slot del coprocessore di sicurezza in base al numero di slot immesso per il controllore primario.

   Se il numero di slot selezionato per il controllore primario non permette il posizionamento del coprocessore di sicurezza immediatamente a destra del controllore primario, verrà richiesto di immettere nuovamente un numero di slot valido.

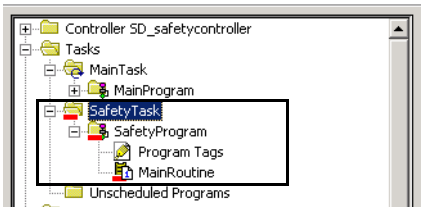


10. Nel menu a discesa Security Authority, selezionare l'opzione per l'authority di sicurezza.

    Per informazioni dettagliate sulla sicurezza, consultare il manuale di programmazione Protezione dei controllori Logix5000, pubblicazione 1756-PM016E-IT-P.
11. Se si desidera utilizzare il livello di protezione selezionato per le operazioni di autenticazione e autorizzazione, contrassegnare la casella al di sotto di Security Authority.
12. Nel campo Description, immettere una descrizione del progetto.
13. Fare clic su Finish.

L'applicazione Logix Designer crea un task di sicurezza e un programma di sicurezza. All'interno del programma di sicurezza viene inoltre creata una routine di sicurezza principale in logica ladder denominata MainRoutine.

Figura 6 – Task di sicurezza nell'organizer del controllore



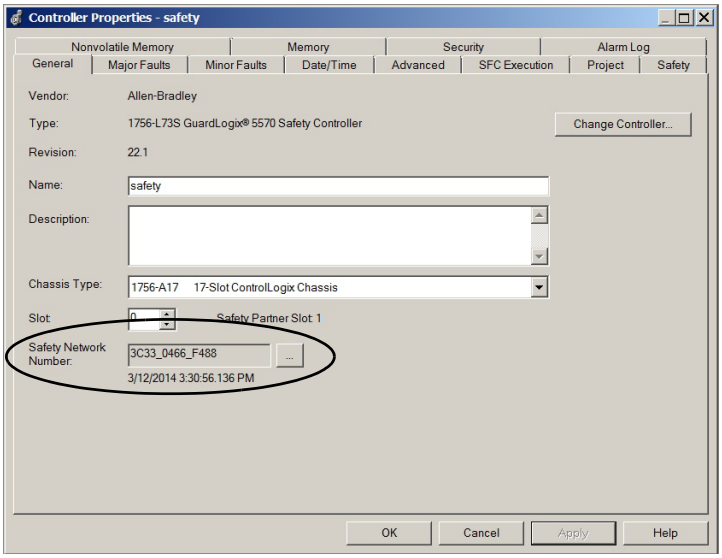
Una barra rossa sotto l'icona consente di distinguere i programmi e le routine di sicurezza dai componenti del progetto standard nell'organizer del controllore.

Quando viene creato un nuovo progetto di sicurezza, l'applicazione Logix Designer genera automaticamente anche un numero rete di sicurezza (SNN, Safety Network Number) basato sul tempo.

Tale valore SNN definisce il backplane dello chassis locale come sottorete di sicurezza. Esso può essere visualizzato e modificato mediante la scheda General nella finestra di dialogo Controller Properties.

Per la maggior parte delle applicazioni, questo numero di rete di sicurezza (SNN) automatico basato sul tempo è sufficiente. Tuttavia esistono dei casi in cui è necessario immettere un SNN specifico.

Figura 7 – Numero della rete di sicurezza



SUGGERIMENTO Per passare da controllore standard a controllore di sicurezza e viceversa, è possibile utilizzare la finestra di dialogo Controller Properties e fare clic sul pulsante Change Controller. Questa azione ha implicazioni sia per i progetti standard sia per quelli di sicurezza.

Per ulteriori informazioni sulle conseguenze del cambiamento dei controllori, vedere Appendice B, Modifica del tipo di controllore.

Tabella 11 - Ulteriori risorse

Risorsa	Descrizione
Capitolo 6, Sviluppo di applicazioni di sicurezza	Contiene ulteriori informazioni su task, programmi e routine di sicurezza.
Capitolo 4, Comunicazione sulle reti	Fornisce ulteriori informazioni sulla gestione del numero SNN.

Codifica elettronica

La codifica elettronica riduce le possibilità di utilizzare un dispositivo errato in un sistema di controllo. La codifica confronta il dispositivo specificato nel progetto con il dispositivo installato. Se la codifica non riesce, viene generato un errore. Vengono confrontati i seguenti attributi.

Attributo	Descrizione
Vendor	Il fabbricante del dispositivo.
Device Type	Il tipo di prodotto in generale: ad esempio, modulo I/O digitale.
Product Code	Il tipo di prodotto specifico. Product Code fa riferimento ad un numero di catalogo.
Major Revision	È un numero che rappresenta le capacità funzionali del dispositivo.
Minor Revision	È un numero che rappresenta le variazioni funzionali del dispositivo.

Sono disponibili le seguenti opzioni di codifica elettronica.

Opzione di codifica	Descrizione
Compatible Module	Permette al dispositivo installato di accettare il codice del dispositivo definito nel progetto qualora il dispositivo installato sia in grado di emulare il dispositivo definito. Tramite l'opzione Compatible Module, è possibile solitamente sostituire un dispositivo con un altro dotato delle seguenti caratteristiche: • Stesso numero di catalogo • Stesso numero di versione o superiore • Per la versione secondaria valgono i seguenti criteri: – Se il numero di versione principale è lo stesso, il numero di versione secondaria deve essere lo stesso o superiore. – Se il numero di versione è superiore, il numero di versione secondaria può essere qualsiasi valore.
Exact Match	Indica che, per impostare la comunicazione, tutti gli attributi di codifica devono corrispondere. Se anche un solo attributo non corrisponde precisamente, la comunicazione con il dispositivo non avviene. L'opzione Exact Match è obbligatoria se si usa Firmware Manager.

Nel selezionare un'opzione di codifica, prendere attentamente in considerazione le implicazioni di tutte le opzioni.

IMPORTANTE Se si modificano i parametri di codifica elettronica online vengono interrotti i collegamenti online al dispositivo e a tutti i dispositivi collegati tramite esso. Inoltre, potrebbero venire interrotti anche i collegamenti dagli altri controllori.

Se il collegamento I/O ad un dispositivo viene interrotto, si potrebbe verificare una perdita di dati.

Ulteriori informazioni

Per informazioni più dettagliate sulla codifica elettronica, vedere la pubblicazione Electronic Keying in Logix5000 Control Systems Application Technique, LOGIX-AT001.

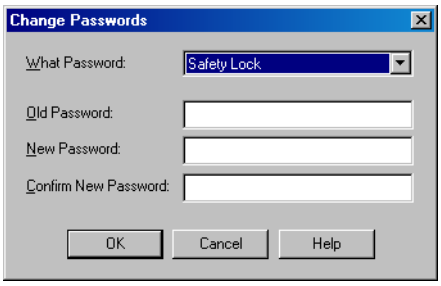
Impostazione delle -password per il blocco/sblocco di sicurezza

Il blocco di sicurezza del controllore contribuisce a proteggere i componenti di controllo di sicurezza dalle modifiche. La funzione di blocco può essere utilizzata solo per i componenti di sicurezza, ad esempio, task, programmi, routine e tag di sicurezza, ma non può essere utilizzata per i componenti standard. Il blocco di sicurezza per il progetto del controllore può essere attivato o disattivato online oppure offline.

La funzione di blocco e sblocco di sicurezza utilizza due password separate. Le password sono opzionali.

Per impostare le password, procedere come indicato di seguito.

1. Fare clic su Tools > Safety > Change Passwords.
2. Dal menu a tendina What Password, selezionare Safety Lock oppure Safety Unlock.



3. Inserire la vecchia password, se esistente.
4. Inserire e confermare la nuova password.
5. Fare clic su OK.

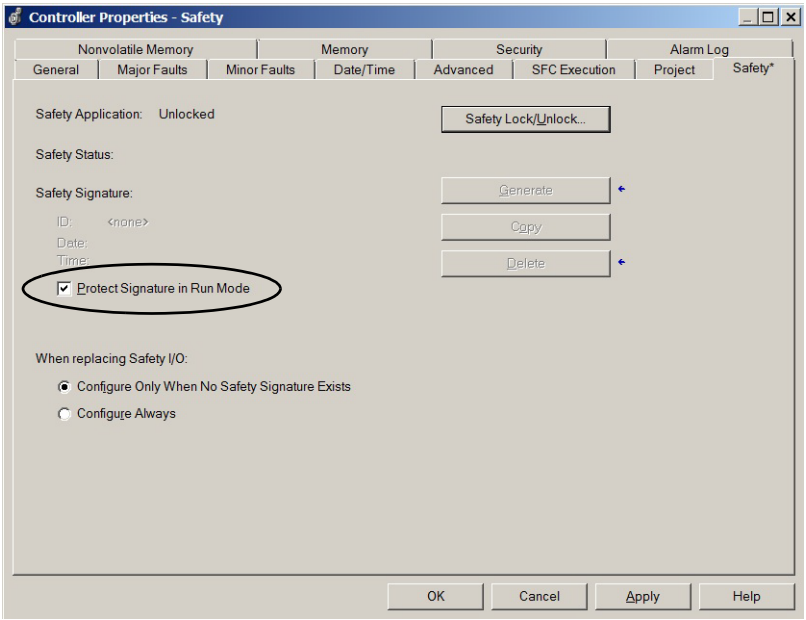
   Le password possono avere una lunghezza compresa tra 1 e 40-caratteri e non vi è distinzione tra maiuscole e minuscole. È possibile utilizzare lettere, valori numerici e i seguenti simboli: ‘ ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? / .

Protezione della firma del task di sicurezza in modalità Esecuzione

È possibile prevenire la creazione o la cancellazione della firma del task di sicurezza mentre il controllore è in modalità Esecuzione o Esecuzione remota, a prescindere dal fatto che l’applicazione di sicurezza sia bloccata o sbloccata.

Per proteggere la firma del task di sicurezza, effettuare le seguenti operazioni:

1. Aprire la finestra di dialogo Controller Properties.
2. Fare clic sulla scheda Safety.
3. Contrassegnare Protect Signature in Run Mode.
4. Fare clic su OK.



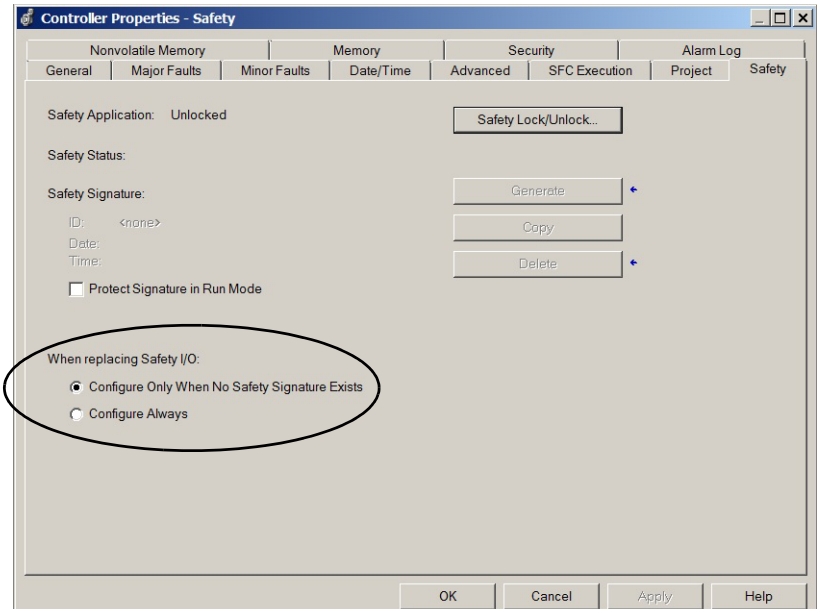
Gestione della sostituzione dei moduli I/O

La scheda Safety della finestra di dialogo Controller Properties consente di definire la modalità di gestione della sostituzione di un dispositivo I/O nel sistema da parte del controllore. Questa opzione determina se il controllore imposta il numero di rete di sicurezza (SSN) di un dispositivo I/O al quale di collega e se dispone dei dati di configurazione qualora esista una firma(1) del task di sicurezza.

Per configurare in che modo il controllore gestisce la sostituzione di un dispositivo I/O nel sistema, procedere come segue.

1. Aprire la finestra di dialogo Controller Properties.
2. Fare clic sulla scheda Safety.
3. Selezionare l'opzione di configurazione per il controllore da usare quando si sostituisce un dispositivo I/O di sicurezza.
4. Fare clic su OK.

Figura 8 – Opzioni di sostituzione del dispositivo I/O



ATTENZIONE: Abilitare l'opzione Configure Always solo se l'intero sistema di controllo di sicurezza CIP instradabile non è utilizzato per mantenere il livello SIL 3 durante la sostituzione e il test funzionale di un dispositivo.

Per ulteriori informazioni, vedere il Capitolo 5, Aggiunta, configurazione, monitoraggio e sostituzione dei dispositivi I/O CIP Safety.

(1) La firma del task di sicurezza è un numero utilizzato per identificare in modo univoco la logica, i dati e la configurazione di ciascun progetto, proteggendo pertanto il livello di integrità di sicurezza del sistema (SIL). Per ulteriori informazioni vedere Firma del task di sicurezza a pagina 14 e Generazione di una firma del task di sicurezza a pagina 102.

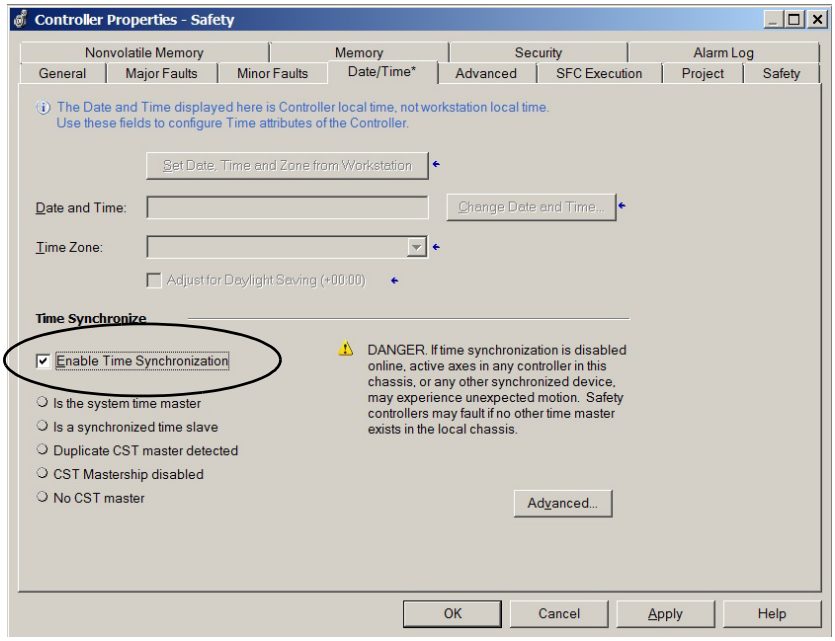
Abilitazione della sincronizzazione temporale

In un sistema di controllo GuardLogix, occorre designare un dispositivo nello chassis locale come master CST (tempo di sistema coordinato). La sincronizzazione temporale è un meccanismo standard per la sincronizzazione degli orologi in una rete di dispositivi distribuiti.

Per configurare il controllore affinché diventi l'unità master CST, procedere come segue.

1. Aprire la finestra di dialogo Controller Properties.
2. Fare clic sulla scheda Date/Time.
3. Selezionare Enable Time Synchronization.
4. Fare clic su OK.

Figura 9 – Scheda Date/Time



Per ulteriori informazioni sulla sincronizzazione temporale, consultare Integrated Architecture and CIP Sync Configuration Application Solution, pubblicazione IA-AT003.

Configurazione di un controllore di sicurezza peer

Per consentire il consumo di tag standard o di sicurezza, è possibile aggiungere un controllore di sicurezza peer alla cartella di configurazione I/O del progetto di sicurezza. Per condividere i dati di sicurezza tra i controllori peer, è possibile produrre e consumare tag di sicurezza definiti nell'ambito del controllore.

Per i dettagli sulla configurazione dei controllori di sicurezza peer e su produzione/consumo dei tag di sicurezza, vedere Tag di sicurezza prodotti/consumati a pagina 92.

Note:

Comunicazione sulle reti

Argomento	Pagina
Rete di sicurezza	47
Comunicazione EtherNet/IP	53
Comunicazione ControlNet	58
Comunicazione DeviceNet	60

Rete di sicurezza

Il protocollo CIP Safety è un protocollo di sicurezza da nodo finale a nodo finale che consente l'instradamento di messaggi CIP Safety da e verso dispositivi I/O di sicurezza tramite bridge, switch e router.

Per mantenere un elevato livello di integrità quando si esegue l'instradamento attraverso bridge, switch o router standard, ciascun nodo finale all'interno di un sistema di controllo CIP safety instradabile deve avere un riferimento univoco. Tale riferimento univoco è una combinazione del numero della rete di sicurezza (SNN) e dell'indirizzo di nodo del dispositivo di rete.

Gestione del numero della rete di sicurezza (SNN)

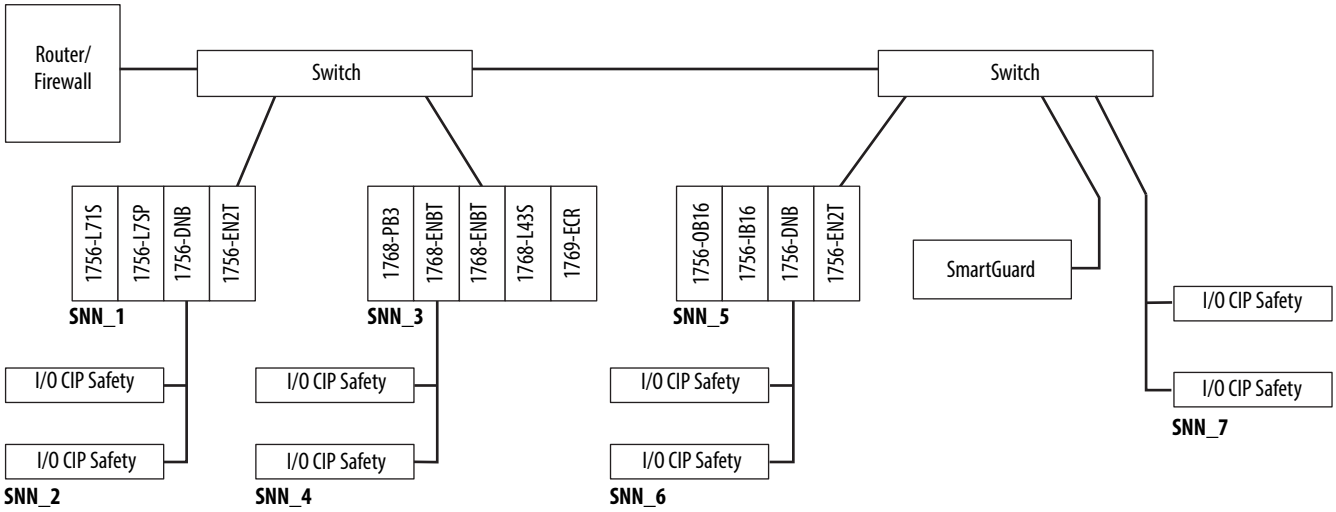
Il valore SNN assegnato ai dispositivi di sicurezza su un segmento di rete deve essere univoco. Accertarsi che ai seguenti elementi sia assegnato un valore SNN univoco:

- Ogni rete CIP safety che contiene dispositivi di sicurezza
- Ogni chassis che contiene uno o più controllori GuardLogix

SUGGERIMENTO Alle sottoreti CIP Safety o agli chassis ControlBus contenenti più di un dispositivo di sicurezza è possibile assegnare più numeri di rete di sicurezza. Tuttavia, per semplicità, si consiglia di utilizzare un unico valore SNN per ciascuna sottorete CIP Safety.

Nella Figura 10 è mostrato un sistema CIP Safety con sette diverse sottoreti, ognuna delle quali dispone di un SNN univoco.

Figura 10 – Esempio CIP Safety con più SNN

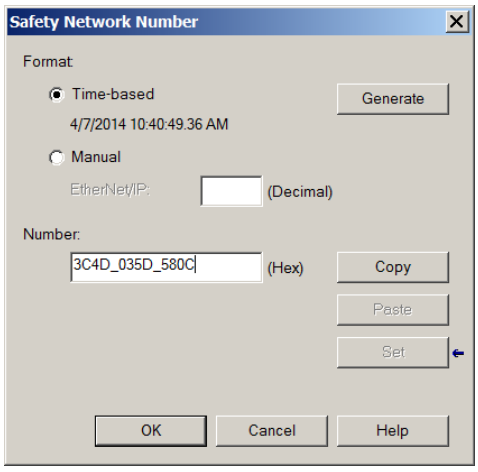


Il valore SNN può essere assegnato dal software (basato sul tempo) oppure dall'utente (manuale). I due formati del valore SNN sono descritti nelle seguenti sezioni.

Numero rete di sicurezza basato sul tempo

Se si seleziona il formato basato sul tempo, il valore SNN indica la data e l'ora in cui il numero è stato generato, in base al computer su cui il software di configurazione è in esecuzione.

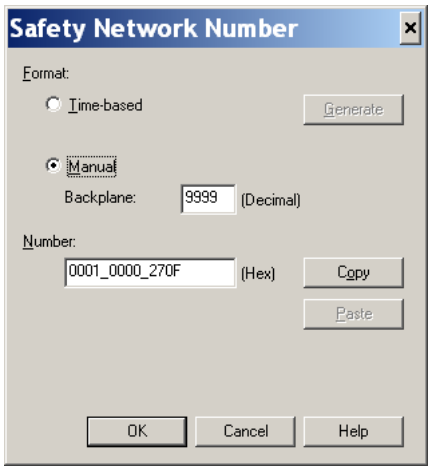
Figura 11 – Formato basato sul tempo



Numero rete di sicurezza manuale

Se viene selezionato il formato manuale, come numero SNN è necessario immettere un valore decimale compreso tra 1 e 9999.

Figura 12 – Immissione manuale



Assegnazione del numero di rete di sicurezza (SNN)

È possibile consentire all'applicazione Logix Designer di assegnare automaticamente un valore SNN, oppure assegnarlo manualmente.

Assegnazione automatica

Quando si crea un controllore o un dispositivo nuovo, viene automaticamente assegnato un numero SNN basato sul tempo. Ai nuovi dispositivi di sicurezza aggiunti successivamente alla stessa rete CIP Safety viene assegnato lo stesso valore SNN definito all'interno dell'indirizzo minimo sulla rete CIP safety.

Assegnazione manuale

L'opzione manuale è destinata ai sistemi CIP Safety instradabili in cui il numero di sottoreti della rete e di reti di interconnessione è minimo e in cui gli utenti possono gestire e assegnare i valori SNN in modo logico in base all'applicazione specifica.

Vedere Modifica del numero di rete di sicurezza (SNN) a pagina 50.

IMPORTANTE

Se si assegna un SNN manualmente, assicurarsi che l'ampliamento del sistema non determini una duplicazione delle combinazioni di SNN e indirizzo di nodo.

In Logix Designer versione 24, se il progetto contiene un valore SNN duplicato e delle combinazioni di indirizzo di nodo duplicate, viene generato un errore.

In Logix Designer versione 26, se il progetto contiene un valore SNN duplicato e delle combinazioni di indirizzo di nodo duplicate, viene visualizzato un avviso. Benché sia comunque possibile verificare il progetto, Rockwell Automation consiglia di risolvere le combinazioni duplicate.

Confronto tra assegnazione automatica e manuale

Per gli utenti tipici, l'assegnazione automatica di un SNN è sufficiente. Tuttavia, la modifica manuale del valore SNN è necessaria nei seguenti casi:

- Se si utilizzano tag di sicurezza consumati.
- Se il progetto consuma i dati di sicurezza in ingresso da un modulo la cui configurazione appartiene ad un altro dispositivo.
- Se il progetto di sicurezza viene copiato in un'altra installazione hardware all'interno dello stesso sistema di sicurezza CIP instradabile.

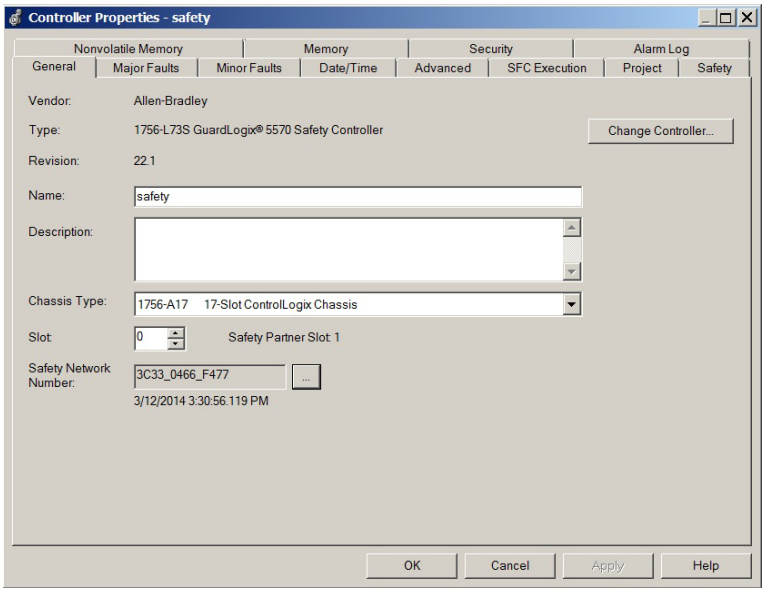
Modifica del numero di rete di sicurezza (SNN)

Prima di modificare il valore SNN, è necessario eseguire le seguenti operazioni:

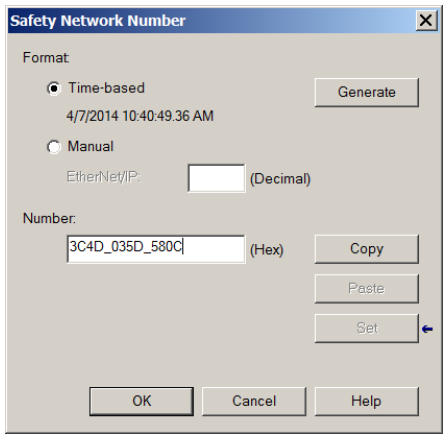
- Sbloccare il progetto, se è in blocco di sicurezza.
  Vedere Blocco di sicurezza del controllore a pagina 100.
- Eliminare la firma del task di sicurezza, se è presente.
  Vedere Eliminazione della firma del task di sicurezza a pagina 103.

Modifica del numero di rete di sicurezza (SNN) del controllore

1. Nell'organizer del controllore, fare clic con il pulsante destro del mouse sul controllore e selezionare Properties.
2. Nella scheda General della finestra di dialogo Controller Properties, fare clic su ... a destra del numero rete di sicurezza per aprire la finestra di dialogo Safety Network Number.



3. Fare clic su Time-based, quindi su Generate.

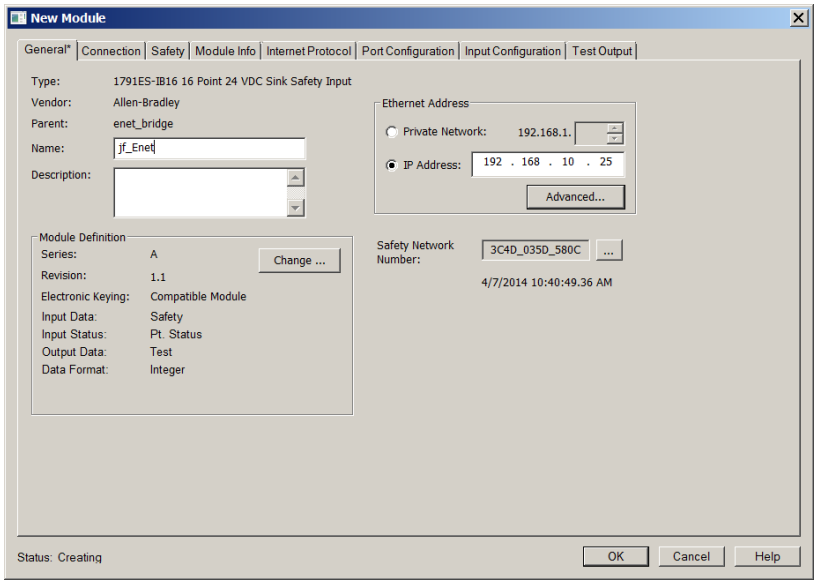


4. Fare clic su OK.

Modifica del numero di rete di sicurezza (SNN) dei dispositivi I/O di sicurezza sulla rete CIP safety

Questo esempio si riferisce ad una rete EtherNet/IP.

1. Ricercare il primo modulo di comunicazione EtherNet/IP nella struttura di configurazione I/O.
2. Espandere i dispositivi I/O di sicurezza disponibili attraverso il modulo di comunicazione EtherNet/IP.
3. Per visualizzare la scheda General, fare doppio clic sul primo dispositivo I/O di sicurezza.



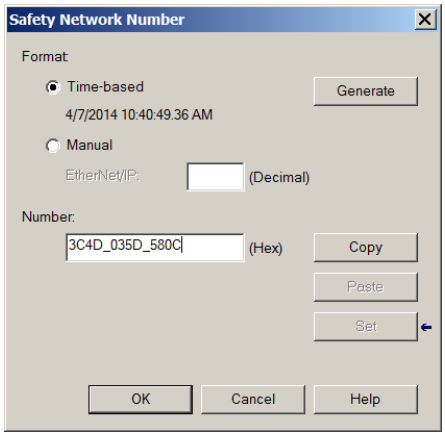
4. Per aprire la finestra di dialogo Safety Network Number, fare clic su ... a destra del numero rete di sicurezza.
5. Per generare un nuovo valore SNN per la rete EtherNet/IP, selezionare Time-based e fare clic su Generate.
6. Fare clic su OK.
7. Per copiare il nuovo valore SNN negli Appunti di Windows, fare clic su Copy.

8. Aprire la scheda General della finestra di dialogo Module Properties del dispositivo I/O di sicurezza successivo del modulo EtherNet/IP specifico.
9. Per aprire la finestra di dialogo Safety Network Number, fare clic su ... a destra del numero rete di sicurezza.
10. Per incollare il valore SNN della rete EtherNet/IP all'interno del dispositivo, selezionare Time-based e fare clic su Paste.
11. Fare clic su OK.
12. Ripetere i passaggi 8-10 per i dispositivi I/O di sicurezza rimanenti nel modulo di comunicazione EtherNet/IP.
13. Ripetere i passi 2...10 per i moduli di comunicazione di rete rimanenti nella struttura di configurazione I/O.

Operazione di copia e incolla di un numero di rete di sicurezza (SNN)

Se la configurazione del modulo appartiene ad un altro controllore, è possibile copiare e incollare il valore SNN dal proprietario della configurazione nel modulo della struttura di configurazione I/O.

1. Nello strumento di configurazione software del proprietario della configurazione del modulo, aprire la finestra di dialogo Safety Network Number relativa al modulo.



2. Fare clic su Copy.
3. Fare clic sulla scheda General nella finestra di dialogo Module Properties del dispositivo I/O nella struttura di configurazione I/O del progetto del controllore consumatore.
   Il controllore consumatore non è il proprietario della configurazione.
4. Per aprire la finestra di dialogo Safety Network Number, fare clic su ... a destra del numero rete di sicurezza.
5. Fare clic su Paste.
6. Fare clic su OK.

Comunicazione EtherNet/IP

Per la comunicazione di rete EtherNet/IP in un sistema GuardLogix, è possibile scegliere tra diversi moduli. Per la comunicazione CIP Safety, comprendente il controllo dei dispositivi I/O di sicurezza, scegliere uno dei moduli elencati nella Tabella 12, tranne il modulo 1756-EWEB, che non supporta la comunicazione CIP Safety.

La Tabella 12 elenca i moduli e le loro funzioni principali.

Tabella 12 – Moduli di comunicazione EtherNet/IP e caratteristiche

Modulo	Caratteristiche
1756-ENBT	• Collegamento dei controllori ai dispositivi I/O (necessità di un adattatore per gli I/O distribuiti). • Comunicazione con altri dispositivi EtherNet/IP (messaggi). • Percorso per la condivisione dei dati tra controllori Logix5000 (produzione/consumo). • Collegamento in ponte dei nodi EtherNet/IP per instradare i messaggi ai dispositivi su altre reti.
1756-EN2T	• Stesse funzioni del modulo 1756-ENBT, ma con capacità doppia per applicazioni più esigenti. • Connessione temporanea per la configurazione tramite porta USB. • Configurazione rapida degli indirizzi IP tramite selettori rotativi.
1756-EN2F	• Stesse funzioni di un modulo 1756-EN2T. • Collegamento dei cavi in fibra tramite un connettore per fibre LC sul modulo.
1756-EN2TXT	• Stesse funzioni di un modulo 1756-EN2T. • Funzionamento in ambienti estremi con temperature comprese nel campo –25…70 °C.
1756-EN2TR	• Stesse funzioni di un modulo 1756-EN2T. • Supporto delle comunicazioni su topologia ad anello per una rete ad anello a livello di dispositivi (DLR, Device Level Ring) a prova di singolo guasto.
1756-EN2TRXT	• Stesse funzioni di un modulo 1756-EN2T. • Supporto delle comunicazioni su topologia ad anello per una rete ad anello a livello di dispositivi (DLR, Device Level Ring) a prova di singolo guasto. • Funzionamento in ambienti estremi con temperature comprese nel campo –25…70 °C.
1756-EN3TR	• Stesse funzioni di un modulo 1756-EN2TR. • Due porte per la connessione DLR.
1756-EWEB	• Pagine Web personalizzabili per l'accesso esterno alle informazioni del controllore. • Accesso remoto, tramite browser Internet, ai tag in un controllore ControlLogix locale. • Comunicazione con altri dispositivi EtherNet/IP (messaggi). • Collegamento in ponte dei nodi EtherNet/IP per instradare i messaggi ai dispositivi su altre reti. • Supporto di dispositivi Ethernet non basati su EtherNet/IP con interfaccia socket. Questo modulo non supporta tag I/O o tag prodotti/consumati né la comunicazione CIP safety.

I moduli di comunicazione EtherNet/IP offrono le seguenti funzioni:

- Supporto messaggistica, tag prodotti/consumati, HMI e I/O distribuiti
- Messaggi incapsulati all'interno del protocollo TCP/UDP/IP standard
- Un livello di applicazione comune con le reti ControlNet e DeviceNet
- Interfaccia mediante cavo a doppino intrecciato, non schermato, RJ45, categoria 5
- Supporto del funzionamento half/full-duplex a 10 M o 100 M
- Funzionamento con switch standard
- Schedulazione di rete non richiesta
- Tabelle di instradamento non richieste

Questi prodotti sono disponibili per le reti EtherNet/IP.

Tabella 13 – Prodotti per moduli EtherNet/IP

Prodotto	Utilizzato per	Necessario
Ambiente Studio 5000	• Configurare il progetto del controllore • Definire la comunicazione EtherNet/IP	Sì
BOOTP/DHCP(1)	Assegnare gli indirizzi IP ai dispositivi su una rete EtherNet/IP	No
Software RSNetWorx for EtherNet/IP	Configurare i dispositivi EtherNet/IP mediante indirizzi IP e/o nomi host	No
Software RSLinx	• Configurare i dispositivi • Stabilire la comunicazione tra i dispositivi • Fornire informazioni di diagnostica	Sì

(1) Disponibile nell'ambiente Studio 5000.

Produzione e consumo dei dati attraverso una rete EtherNet/IP

Il controllore supporta la produzione (invio) e il consumo (ricezione) dei tag su una rete Ethernet/IP. Tutti i tag prodotti e consumati richiedono connessioni. Il numero totale di tag producibili e consumabili è limitato dal numero di connessioni disponibili.

Connessioni sulla rete EtherNet/IP

Configurando il controllore di sicurezza per la comunicazione con altri dispositivi nel sistema, si determina indirettamente il numero di connessioni utilizzate dal controllore. Le connessioni sono allocazioni di risorse che garantiscono una comunicazione tra i dispositivi più affidabile se paragonata ai messaggi non connessi (istruzioni di messaggio).

Le connessioni EtherNet/IP non sono schedulate. Una connessione non schedulata viene attivata dall'intervallo di pacchetto richiesto (RPI, Requested Packet Interval) per il controllo I/O o dal programma (ad esempio un'istruzione MSG). La messaggistica non schedulata consente di inviare e ricevere i dati quando necessario.

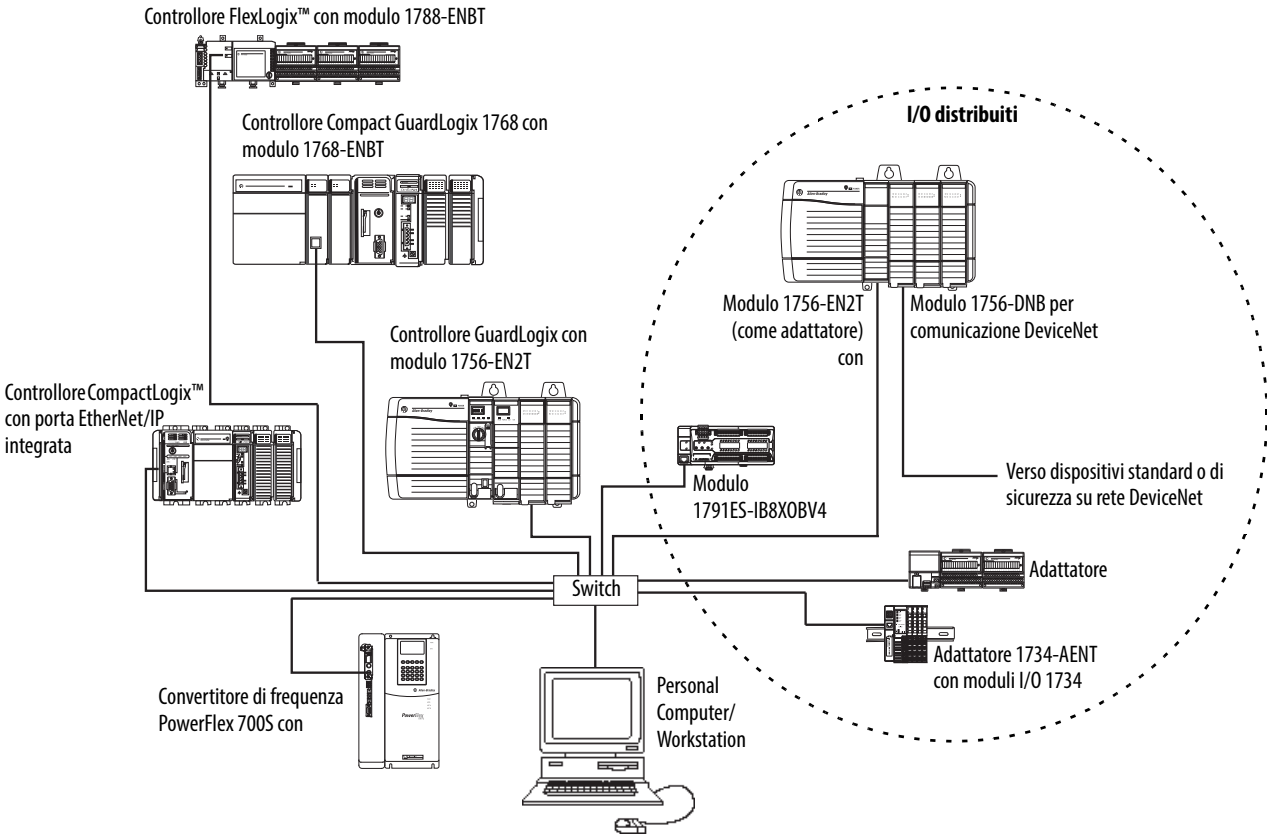
I moduli di comunicazione EtherNet/IP supportano 128 connessioni CIP (Common Industrial Protocol) su una rete EtherNet/IP.

Esempi di comunicazione EtherNet/IP

La Figura 13 illustra le seguenti funzioni di comunicazione:

- I controllori possono produrre e consumare tra loro tag standard o di sicurezza.
- I controllori possono generare istruzioni MSG che inviano/ricevono dati standard o configurano dispositivi.(1)
- Il modulo di comunicazione EtherNet/IP può essere utilizzato come bridge, consentendo al controllore di sicurezza di produrre e consumare dati standard e di sicurezza.
- La workstation può eseguire upload/download di progetti sui controllori.
- La workstation può configurare i dispositivi sulla rete EtherNet/IP.

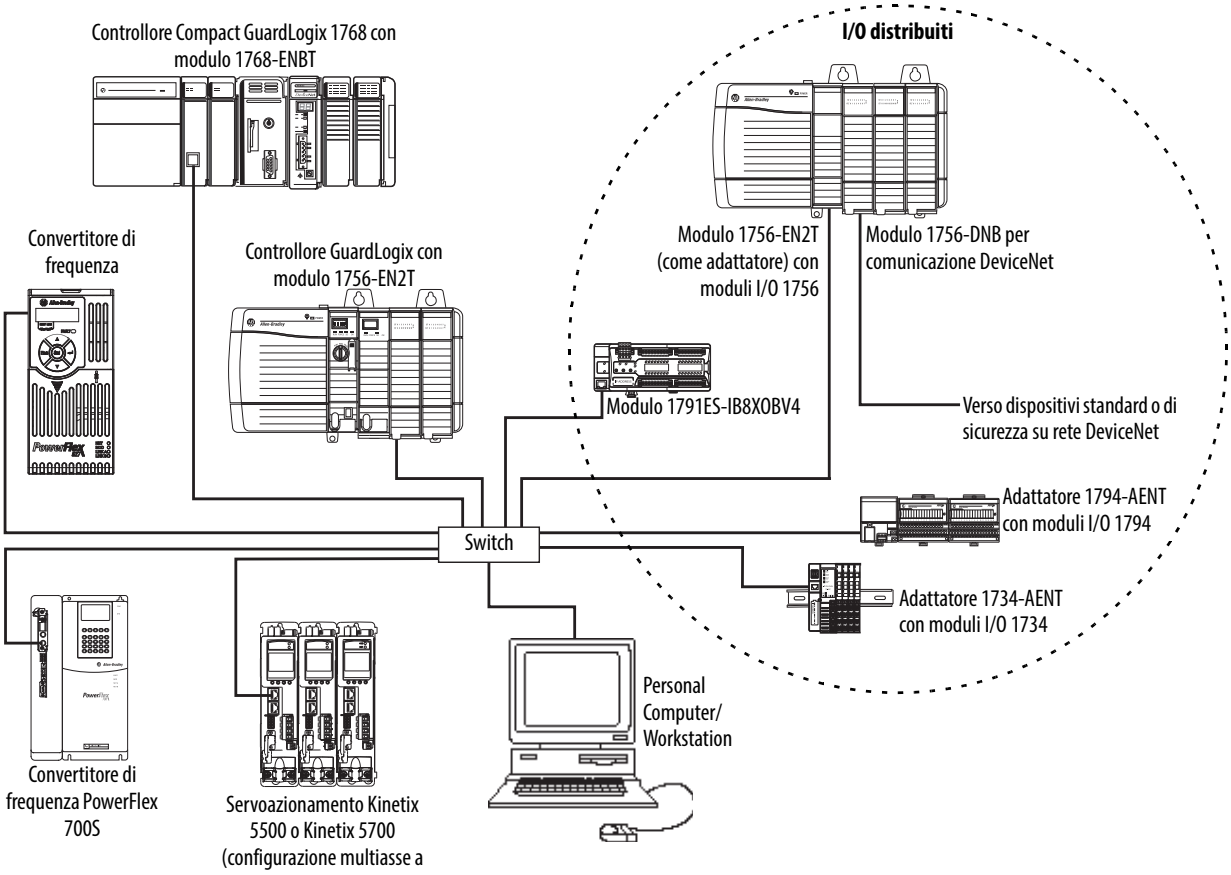
Figura 13 – Esempio di comunicazione EtherNet/IP



(1) I controllori GuardLogix non supportano le istruzioni MSG per i dati di sicurezza.

Nell'applicazione Logix Designer, versione 24 e successive, il controllore supporta sia connessioni standard che di sicurezza tramite una sola connessione.

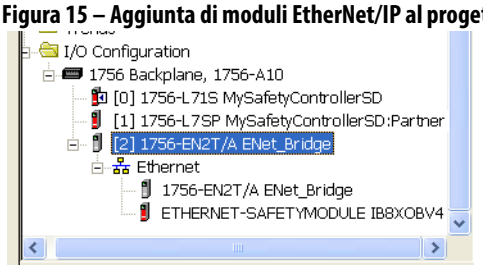
Figura 14 – Esempio di comunicazione EtherNet/IP con connessione standard e di sicurezza



Connessioni EtherNet/IP per dispositivi I/O di sicurezza

I dispositivi I/O di sicurezza su reti EtherNet/IP vengono aggiunti al progetto nel modulo di comunicazione EtherNet/IP, come descritto in Aggiunta di dispositivi I/O di sicurezza a pagina 63. Quando si aggiunge un dispositivo di sicurezza I/O, l'applicazione Logix Designer crea automaticamente per tale dispositivo dei tag di dati di sicurezza definiti nell'ambito del controllore.

Figura 15 – Aggiunta di moduli EtherNet/IP al progetto



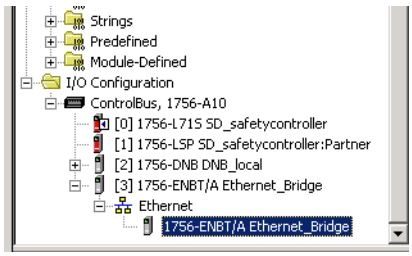
Connessioni EtherNet/IP standard

Per utilizzare un modulo EtherNet/IP standard con il controllore di sicurezza, è necessario aggiungere il modulo al progetto del controllore di sicurezza e scaricare il progetto nel controllore GuardLogix.

1. Per configurare il modulo, definire indirizzo IP, maschera di sottorete e gateway.

Parametro EtherNet/IP	Descrizione
indirizzo IP	L'indirizzo IP identifica il modulo in modo univoco. L'indirizzo IP si presenta nella forma *xxx.xxx.xxx.xxx.* dove ogni xxx corrisponde ad un numero compreso tra 0 e 255. Tuttavia, vi sono alcuni valori che non possono essere utilizzati come primo ottetto dell'indirizzo: • 000.*xxx.xxx.xxx* • 127.*xxx.xxx.xxx* • 223…255.*xxx.xxx.xxx*
Maschera di sottorete	L'indirizzamento della sottorete è un'estensione dello schema dell'indirizzo IP che consente ad un sito di utilizzare un solo ID di rete per più reti fisiche. L'instradamento all'esterno del sito continua suddividendo l'indirizzo IP in un ID di rete e in un ID host tramite la classe. All'interno di un sito, la maschera di sottorete è utilizzata per suddividere l'indirizzo IP in un ID di rete personalizzato e in un ID host. Per default, questo campo è impostato su 0.0.0.0. Se si modifica la maschera di sottorete di un modulo già configurato, è necessario spegnere e riaccendere perché la modifica diventi attiva.
Gateway	Il gateway connette singole reti fisiche in un sistema di reti. Quando un nodo deve comunicare con un nodo su un'altra rete, il gateway trasferisce i dati tra le due reti. Per default, questo campo è impostato su 0.0.0.0.

2. Dopo avere installato fisicamente un modulo EtherNet/IP e impostato il relativo indirizzo IP, è necessario aggiungere il modulo all'organizer del controllore nel progetto del controllore GuardLogix.



3. Usare l'applicazione Logix Designer per scaricare il progetto.

Comunicazione ControlNet

Per le comunicazioni ControlNet, scegliere un modulo 1756-CNB o 1756-CNBR per comunicazioni standard, oppure un modulo 1756-CN2, 1756-CN2R o 1756-CN2RXT per comunicazioni di sicurezza.

Tabella 14 – Moduli ControlNet

Se l'applicazione	Selezionare
• Controlla i dispositivi I/O standard • Necessita di un adattatore per I/O distribuiti sui link ControlNet • Comunica con altri dispositivi ControlNet (messaggi) • Condivide dati standard con altri controllori Logix5000 (produzione/consumo) • Funge da bridge con i link ControlNet per instradare i messaggi a dispositivi su altre reti	1756-CNB
• Svolge le stesse funzioni di un modulo 1756-CNB • È compatibile anche con i supporti ControlNet ridondanti	1756-CNBR
• Svolge le stesse funzioni supportate dal modulo 1756-CNB con prestazioni superiori • Supporta la comunicazione CIP Safety	1756-CN2
• Svolge le stesse funzioni di un modulo 1756-CN2 • È compatibile anche con i supporti ControlNet ridondanti	1756-CN2R
• Esegue le stesse funzioni di un modulo 1756-CN2R • Funziona in ambienti estremi con temperature di –25…70 °C	1756-CN2RXT

Questi prodotti sono disponibili per le reti ControlNet.

Tabella 15 – Prodotti per moduli ControlNet

Prodotto	Utilizzato per	Necessario
Ambiente Studio 5000	• Configurare il progetto GuardLogix • Definire la comunicazione ControlNet	Sì
Software RSNetWorx for ControlNet	• Configurare la rete ControlNet • Definire il tempo di aggiornamento della rete (NUT) • Schedulare la rete ControlNet	Sì
Software RSLinx	• Configurare i dispositivi • Stabilire la comunicazione tra i dispositivi • Fornire informazioni di diagnostica	Sì

I moduli di comunicazione ControlNet forniscono quanto segue:

- Supportano messaggistica, tag standard e di sicurezza prodotti/consumati e I/O distribuiti
- Supportano l'utilizzo di ripetitori con cavi coassiali o fibre ottiche per consentire l'isolamento e l'aumento della distanza.

Produzione e consumo dei dati attraverso una rete ControlNet

Il controllore GuardLogix supporta la produzione (invio) e il consumo (ricezione) dei tag su reti ControlNet. Il numero totale di tag producibili o consumabili è limitato dal numero di connessioni disponibili nel controllore GuardLogix.

Connessioni sulla rete ControlNet

Configurando il controllore per la comunicazione con altri dispositivi nel sistema, si determina il numero di connessioni utilizzate dal controllore. Le connessioni sono allocazioni di risorse che garantiscono una comunicazione tra i dispositivi più affidabile se paragonata ai messaggi non connessi.

Le connessioni ControlNet possono essere schedulate o non schedulate.

Tabella 16 – Connessioni ControlNet

Tipo di collegamento	Descrizione
Schedulato (univoca per la rete ControlNet)	Una connessione schedulata è univoca per la comunicazione ControlNet. Questo tipo di connessione consente di inviare e ricevere dati ripetutamente in base ad un intervallo prestabilito, corrispondente all'intervallo di pacchetto richiesto (RPI, Requested Packet Interval). Ad esempio, una connessione ad un dispositivo I/O è una connessione schedulata, poiché vengono ricevuti ripetutamente dati dal modulo ad intervalli specifici. Altri tipi di connessioni schedulate includono le connessioni a: • Dispositivi di comunicazione • Tag prodotti/consumati Su una rete ControlNet, per abilitare le connessioni schedulate e stabilire un tempo di aggiornamento della rete (NUT, Network Update Time), occorre utilizzare il software RSNetWorx for ControlNet. La schedulazione di una connessione riserva una larghezza di banda della rete per la gestione specifica della connessione.
Non schedulato	Una connessione non schedulata è un trasferimento di messaggi tra controllori che viene attivato dall'intervallo di pacchetto richiesto (RPI, Requested Packet Interval) o dal programma (ad esempio un'istruzione MSG). La messaggistica non schedulata consente di inviare e ricevere i dati quando necessario. Le connessioni non schedulate utilizzano la larghezza di banda della rete rimanente dopo l'allocazione delle connessioni schedulate. Le connessioni di sicurezza prodotte/consumate non sono schedulate.

I moduli di comunicazione 1756-CNB e 1756-CNBR supportano 64 connessioni CIP su una rete ControlNet. Tuttavia, è consigliabile configurare non più di 48 connessioni per mantenere le prestazioni ottimali.

Il modulo 1756-CN2 supporta 128 connessioni CIP sulla rete ControlNet.

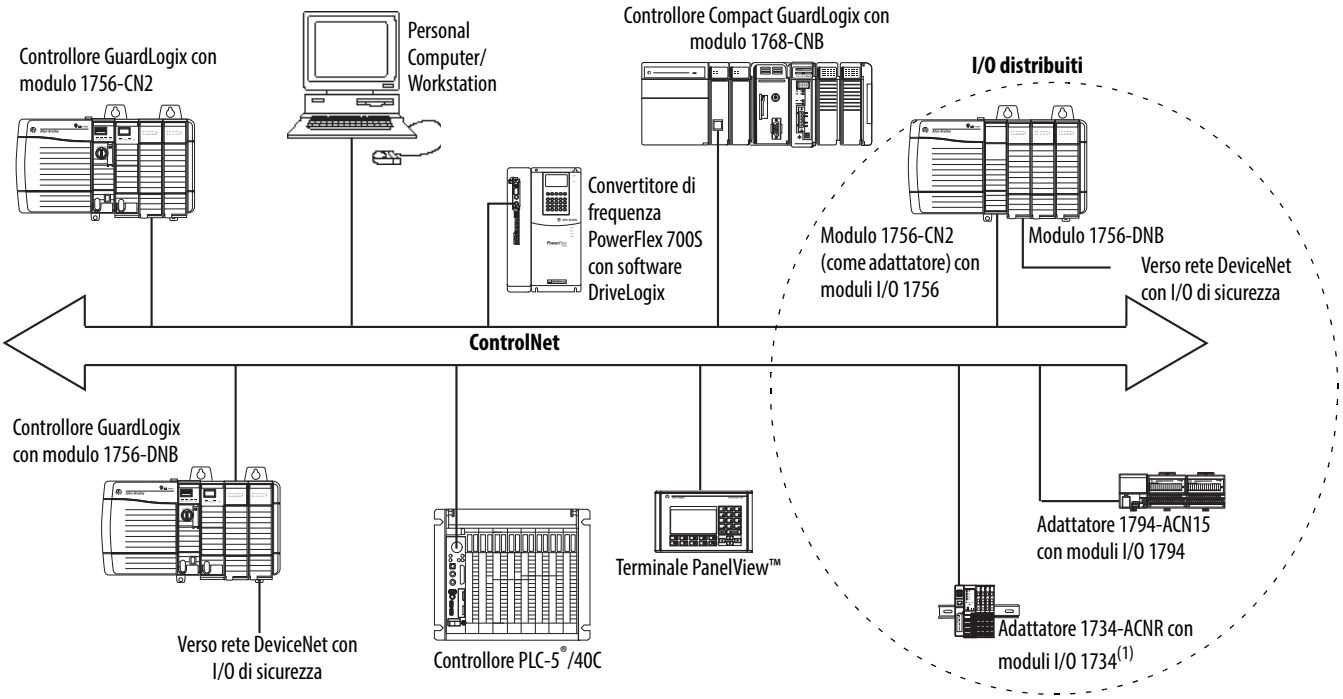
Esempio di comunicazione ControlNet

Questo esempio illustra quanto segue:

- I controllori GuardLogix possono produrre e consumare tra loro tag standard o di sicurezza.
- GuardLogix I controllori possono generare istruzioni MSG che inviano/ricevono dati standard o configurano dispositivi.(1)
- Il modulo 1756 -CN2 può essere utilizzato come bridge, per consentire al controllore GuardLogix di produrre e consumare dati standard e di sicurezza da e verso dispositivi I/O.
- Il personal computer può eseguire upload/download di progetti nei controllori.
- Il personal computer può configurare dispositivi sulla rete ControlNet, nonché la rete stessa.

(1) I controllori GuardLogix non supportano le istruzioni MSG per i dati di sicurezza.

Figura 16 – Esempio di comunicazione ControlNet



(1) L'adattatore 1734-ACN non supporta i moduli I/O di sicurezza POINT Guard I/O.

Connessioni ControlNet per I/O distribuiti

Per comunicare con i dispositivi I/O distribuiti in una rete ControlNet, è necessario aggiungere un bridge ControlNet, un adattatore ControlNet e dispositivi I/O nella cartella di configurazione I/O del controllore.

Comunicazione DeviceNet

Per comunicare e scambiare dati con i dispositivi I/O di sicurezza su reti DeviceNet, è necessario un modulo 1756-DNB nello chassis locale.

Per informazioni sulla modalità di installazione del modulo 1756-DNB, fare riferimento alle istruzioni per l'installazione ControlLogix DeviceNet Scanner Module, pubblicazione 1756-IN566.

Il modulo 1756-DNB supporta la comunicazione con i dispositivi DeviceNet Safety e DeviceNet standard. Pertanto, è possibile utilizzare entrambe le tipologie.

Questi prodotti vengono utilizzati con le reti DeviceNet e il modulo 1756-DNB.

Tabella 17 – Prodotti da utilizzare con le reti DeviceNet

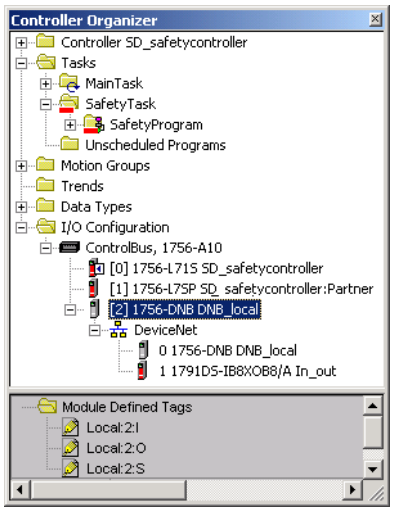
Prodotto	Utilizzato per	Necessario
Ambiente Studio 5000	• Configurare progetti ControlLogix. • Definire la comunicazione DeviceNet.	Sì
Software RSNetWorx for DeviceNet	• Configurare i dispositivi DeviceNet. • Definire l'elenco di scansione per tali dispositivi.	Sì
Software RSLinx Classic o RSLinx Enterprise	• Configurare i dispositivi di comunicazione. • Eseguire attività di diagnostica. • Attivare le comunicazioni tra i dispositivi.	Sì

Connessioni DeviceNet per dispositivi I/O di sicurezza

Per accedere ai dispositivi di sicurezza sulle reti DeviceNet, aggiungere un modulo 1756-DNB alla struttura di configurazione I/O del progetto del controllore GuardLogix.

I dispositivi I/O di sicurezza sulle reti DeviceNet vengono aggiunti al progetto nel modulo 1756-DNB, come descritto al Capitolo 5, Aggiunta, configurazione, monitoraggio e sostituzione dei dispositivi I/O CIP Safety. Quando si aggiunge un dispositivo di sicurezza I/O, l'applicazione Logix Designer crea automaticamente per tale dispositivo dei tag di dati di sicurezza definiti nell'ambito del controllore.

Figura 17 – Modulo DeviceNet nel controllore nella struttura di configurazione I/O



Connessioni DeviceNet standard

Se si utilizzano I/O DeviceNet standard con il controllore GuardLogix, è necessario allocare due connessioni per ciascun modulo 1756-DNB: una connessione è per lo stato del modulo e la configurazione, mentre l'altra è una connessione ottimizzata per rack per i dati I/O DeviceNet.

Per utilizzare il modulo 1756-DNB per l'accesso ai dati standard tramite la rete DeviceNet, è necessario utilizzare il software RSNetWorx for DeviceNet per eseguire le seguenti operazioni:

- Creare un file di configurazione per la rete.
- Configurare ciascun dispositivo standard sulla rete.
- Configurare il modulo 1756-DNB.
- Aggiungere dispositivi I/O standard all'elenco di scansione 1756-DNB.

Quando si aggiunge il modulo 1756-DNB alla configurazione I/O del controllore, l'applicazione Logix Designer crea automaticamente un gruppo di tag standard per i dati di ingresso, uscita e di stato della rete.

Note:

Aggiunta, configurazione, monitoraggio e sostituzione dei dispositivi I/O CIP Safety

Argomento	Pagina
Aggiunta di dispositivi I/O di sicurezza	63
Configurazione dei dispositivi I/O di sicurezza	64
Impostazione dell'indirizzo IP tramite il sistema di traduzione degli indirizzi di rete (NAT)	65
Impostazione del numero rete di sicurezza (SNN)	67
Utilizzo delle connessioni unicast su reti EtherNet/IP	67
Impostazione del limite del tempo di risposta della connessione	67
Comprensione dell'autenticazione di configurazione	71
Ripristino della proprietà dei dispositivi I/O di sicurezza	72
Indirizzamento dei dati I/O di sicurezza	72
Monitoraggio dello stato dei dispositivi I/O di sicurezza	74
Reset di un modulo alle condizioni predefinite in fabbrica	75
Sostituzione di un dispositivo utilizzando l'applicazione Logix Designer	75
Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet	81

Per ulteriori informazioni sull'installazione, la configurazione e l'utilizzo dei dispositivi I/O di sicurezza, consultare Per ulteriori informazioni a pagina 11.

Aggiunta di dispositivi I/O di sicurezza

Se si aggiunge un dispositivo I/O di sicurezza al sistema, è necessario definire una configurazione per il dispositivo, comprendente i seguenti elementi:

- Indirizzo del nodo per reti DeviceNet

  Non è possibile configurare l'indirizzo di nodo di un dispositivo I/O di sicurezza sulle reti DeviceNet mediante l'applicazione Logix Designer. Gli indirizzi di nodo devono essere impostati tramite selettori rotativi sui dispositivi.
- Indirizzo IP per reti EtherNet/IP

  Per impostare l'indirizzo IP è possibile regolare i selettori rotativi sul dispositivo, utilizzare il software DHCP (fornito da Rockwell Automation), utilizzare l'applicazione Logix Designer oppure recuperare l'indirizzo predefinito dalla memoria non volatile.
- Numero della rete di sicurezza (SNN)

  Per informazioni sull'impostazione del valore SNN, vedere a pagina 67.
- Autenticazione di configurazione

  Per informazioni sulle modalità di impostazione automatica o manuale dell'autenticazione di configurazione, vedere a pagina 71.

- Limite del tempo di risposta

  Per informazioni sull'impostazione del limite del tempo di risposta, vedere a pagina 67.
- La configurazione del modulo viene completata con i parametri di test, uscita e ingresso di sicurezza

Per configurare i dispositivi I/O di sicurezza tramite il controllore GuardLogix è possibile utilizzare l'applicazione Logix Designer.

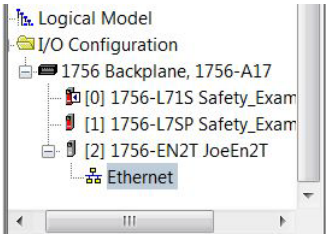
SUGGERIMENTO I dispositivi I/O di sicurezza supportano dati standard e di sicurezza. La configurazione dei dispositivi determina i dati disponibili.

Configurazione dei dispositivi I/O di sicurezza

Il dispositivo I/O di sicurezza deve essere aggiunto al modulo di comunicazione nella cartella di configurazione I/O del progetto del controllore.

SUGGERIMENTO Non è possibile aggiungere o eliminare un dispositivo I/O di sicurezza mentre è online.

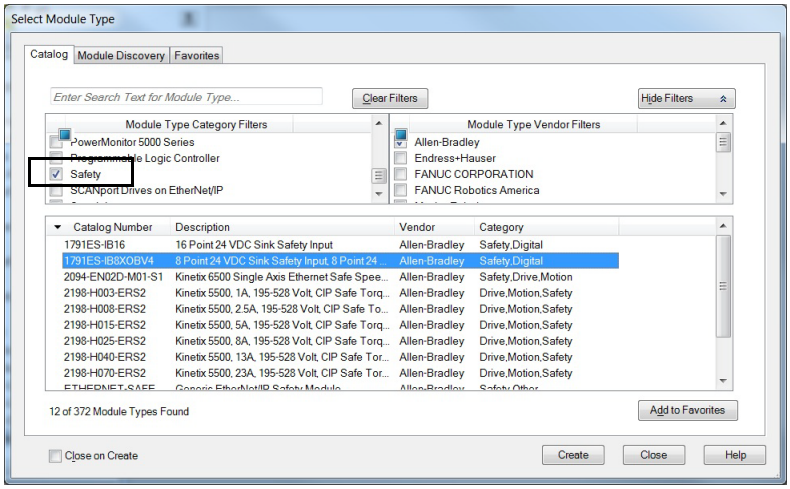
1. Fare clic con il pulsante destro del mouse sulla rete DeviceNet o Ethernet e selezionare New Module.



Questo esempio si riferisce ad una rete Ethernet.

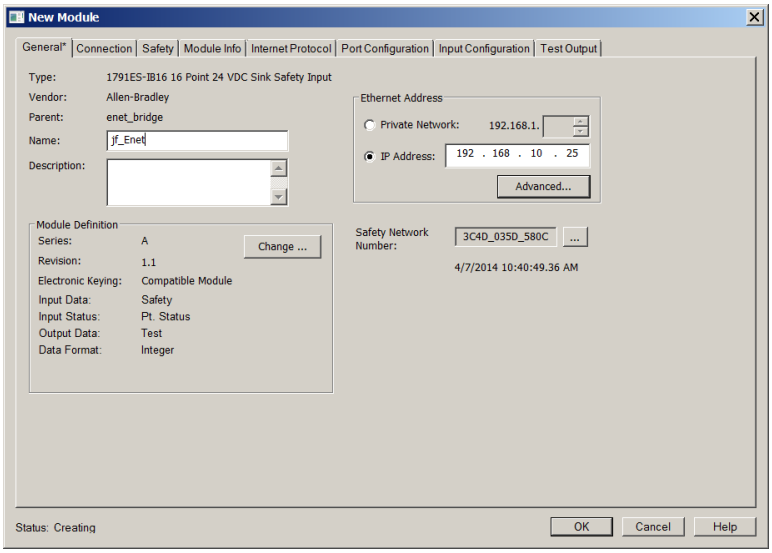
2. Nella scheda Catalog, selezionare il dispositivo I/O di sicurezza.

SUGGERIMENTO Per ridurre l'elenco di moduli tra cui scegliere, utilizzare i filtri.



3. Fare clic su Create.

4. Immettere un nome per il nuovo dispositivo.



5. Se è necessario modificare le impostazioni Module Definition, fare clic su Change.
6. Per le reti DeviceNet immettere l'indirizzo del nodo oppure per le reti EtherNet/IP immettere l'indirizzo IP.

   Nel menu a tendina sono inclusi solo i numeri di nodo non utilizzati.

   Se la rete utilizza il sistema di traduzione degli indirizzi di rete (NAT), vedere Impostazione dell'indirizzo IP tramite il sistema di traduzione degli indirizzi di rete (NAT) a pagina 65.
7. Se è necessario modificare il numero di rete di sicurezza, fare clic sul pulsante ...

   Per ulteriori informazioni, vedere a pagina 67.
8. Impostare il limite del tempo di risposta della connessione utilizzando la scheda Safety.

   Per ulteriori informazioni, vedere a pagina 67.
9. Per completare la configurazione del dispositivo I/O di sicurezza, consultare la relativa documentazione per l'utente e la guida online dell'applicazione Logix Designer.

Impostazione dell'indirizzo IP tramite il sistema di traduzione degli indirizzi di rete (NAT)

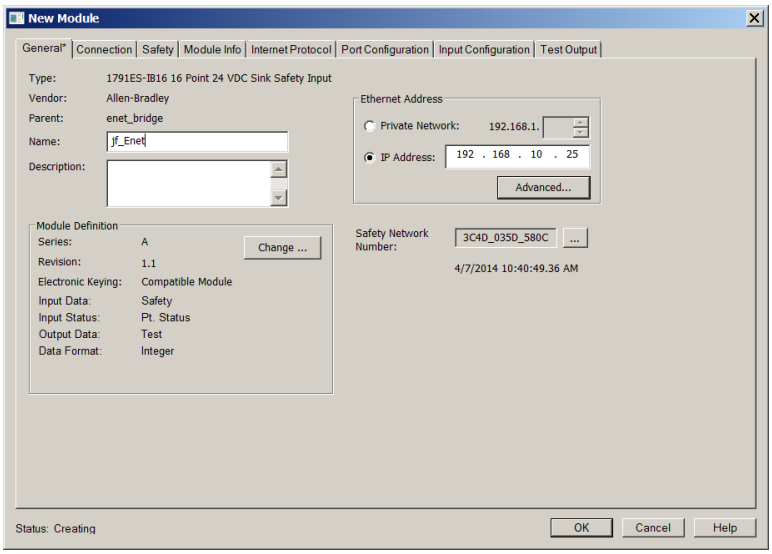
Il sistema NAT traduce un indirizzo IP in un altro indirizzo IP tramite un router o uno switch con configurazione NAT. Il router o lo switch traducono gli indirizzi di origine e di destinazione all'interno dei pacchetti di dati non appena il traffico passa tra le sottoreti.

Questo servizio è utile se è necessario riutilizzare gli indirizzi IP in una rete. Ad esempio, NAT consente di segmentare i dispositivi in più sottoreti private identiche mantenendo allo stesso tempo le identità univoche sulla sottorete pubblica.

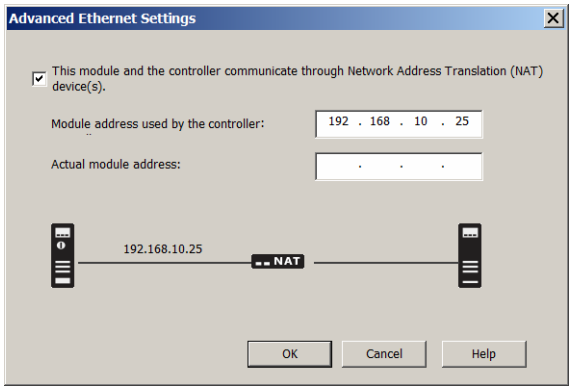
Per impostare l'indirizzo IP tramite il sistema NAT, procedere come segue.

1. Nel campo IP Address immettere l'indirizzo IP che verrà utilizzato dal controllore.

   Quando si utilizza NAT, questo è solitamente l'indirizzo IP sulla rete pubblica.



2. Fare clic su Advanced per aprire la finestra di dialogo Advanced Ethernet Settings.



3. Contrassegnare la casella di controllo per indicare che questo modulo e il controllore comunicano tramite dispositivi NAT.
4. Immettere l'indirizzo nel campo Actual module address.

SUGGERIMENTO Se si configura l'indirizzo IP tramite i selettori rotativi, in questo campo è necessario immettere l'indirizzo impostato sul dispositivo. In caso contrario, nel campo Actual module address occorre immettere lo stesso indirizzo presente sulla scheda Internet Protocol del dispositivo.

5. Fare clic su OK.

Il controllore utilizza l'indirizzo tradotto, ma il protocollo CIP Safety richiede l'indirizzo reale del dispositivo.

Impostazione del numero rete di sicurezza (SNN)

Quando si aggiungono nuovi dispositivi I/O di sicurezza, l'assegnazione di un valore SNN basato sul tempo è automatica. Ai dispositivi di sicurezza aggiunti successivamente alla stessa rete viene assegnato lo stesso valore SNN definito all'interno dell'indirizzo minimo sulla rete CIP Safety.

Per la maggior parte delle applicazioni, questo valore SNN basato sul tempo e automatico è sufficiente. Tuttavia, in alcuni casi è necessario modificare un valore SNN.

Vedere Assegnazione del numero di rete di sicurezza (SNN) a pagina 49.

Utilizzo delle connessioni unicast su reti EtherNet/IP

Le connessioni unicast sono connessioni punto a punto tra un nodo sorgente e un nodo di destinazione. Per questo tipo di connessione, non bisogna inserire un campo RPI minimo o massimo o un valore predefinito.

Per configurare le connessioni unicast, accedere alla scheda Connection e selezionare Use Unicast Connection over EtherNet/IP.

Impostazione del limite del tempo di risposta della connessione

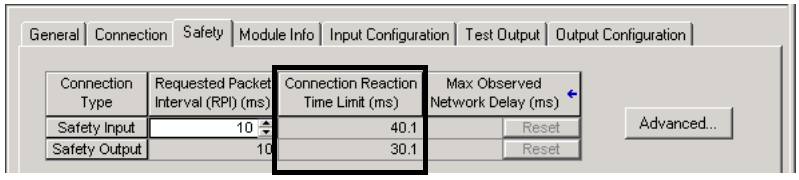
Il limite del tempo di risposta della connessione è la durata massima dei pacchetti di sicurezza sulla connessione associata. Se la durata dei dati utilizzati dal dispositivo consumatore è superiore al limite del tempo di risposta della connessione, si verifica un errore di connessione. Il limite del tempo di risposta della connessione è determinato tramite le seguenti equazioni:

Limite del tempo di risposta della connessione in ingresso =
RPI ingresso x [Moltiplicatore timeout + Moltiplicatore ritardo rete]

Limite del tempo di risposta della connessione in uscita =
Periodo del task di sicurezza x [Moltiplicatore timeout + Moltiplicatore ritardo rete – 1]

Il limite del tempo di risposta della connessione è visualizzato nella scheda Safety della finestra di dialogo Module Properties.

Figura 18 – Limite del tempo di risposta della connessione



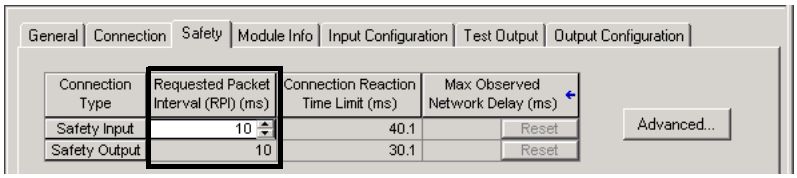
Impostazione dell'intervallo di pacchetto richiesto (RPI)

L'intervallo RPI specifica l'intervallo tra gli aggiornamenti dei dati su una connessione. Ad esempio, un modulo di ingresso produce dati secondo l'intervallo RPI assegnato.

Per le connessioni di ingresso di sicurezza, è possibile impostare l'intervallo RPI nella scheda Safety della finestra di dialogo Module Properties. L'intervallo RPI viene inserito per incrementi di 1 ms, in un intervallo compreso tra 1 e 100 ms. L'impostazione predefinita è 10 ms.

Quando l'intervallo RPI viene modificato tramite l'applicazione Logix Designer, il parametro del limite del tempo di risposta della connessione viene immediatamente regolato.

Figura 19 – Intervallo di pacchetto richiesto



Per le connessioni di uscita di sicurezza, l'intervallo RPI è fissato al periodo del task di sicurezza. Se il limite del tempo di risposta della connessione corrispondente non è soddisfacente, è possibile regolare il periodo del task di sicurezza dalla finestra di dialogo Safety Task Properties.

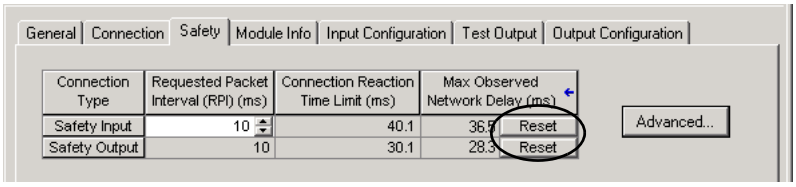
Per ulteriori informazioni sul periodo del task di sicurezza, vedere Definizione del periodo del task di sicurezza a pagina 86.

Per applicazioni normali, l'intervallo RPI predefinito è generalmente sufficiente. Per requisiti più complessi, utilizzare il pulsante Advanced per modificare i parametri di Connection Reaction Time Limit, come descritto a pagina 69.

Visualizzazione del ritardo rete massimo osservato

Quando il controllore GuardLogix riceve un pacchetto di sicurezza, il software registra il ritardo di rete massimo osservato. Nel caso degli ingressi di sicurezza, in corrispondenza di Maximum Observed Network Delay viene visualizzato il ritardo del percorso dal modulo di ingresso al controllore e del ritorno della conferma al modulo di ingresso. Nel caso delle uscite di sicurezza, viene visualizzato il ritardo del percorso dal controllore al modulo di uscita e del ritorno della conferma al controllore. Il parametro Maximum Observed Network Delay è mostrato nella scheda Safety della finestra di dialogo Module Properties. Se si è online, fare clic su Reset per ripristinare il massimo ritardo di rete osservato.

Figura 20 – Reset del massimo ritardo di rete osservato

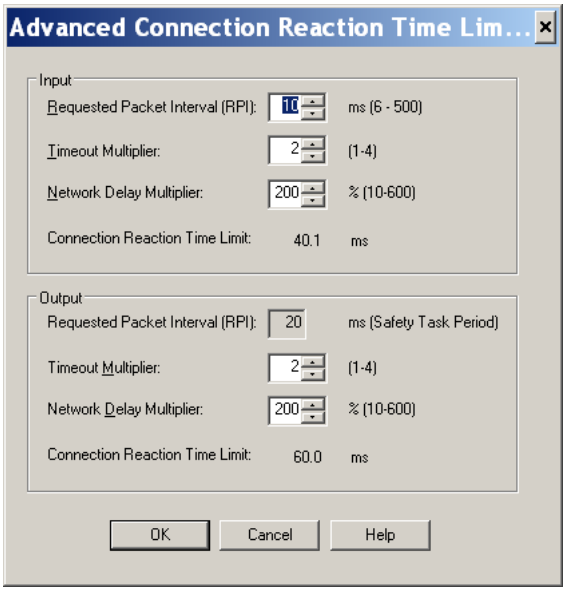


IMPORTANTE Il ritardo di rete massimo effettivo dal produttore al consumatore è inferiore al valore visualizzato nel campo Maximum Network Delay della scheda Safety. In generale, il ritardo massimo effettivo dei messaggi è pari a circa la metà del valore Maximum Network Delay visualizzato.

Impostazione dei parametri avanzati relativi ai limiti del tempo di risposta della connessione

Configurare i parametri di connessione, come Timeout Multiplier e Network Delay Multiplier nella finestra di dialogo Advanced Connection Reaction Time Limit.

Figura 21 – Configurazione avanzata



Timeout Multiplier

Il parametro Timeout Multiplier determina il numero di RPI di attesa di un pacchetto prima di dichiarare il timeout della connessione. Ciò si traduce nel numero di messaggi che possono andare persi prima che venga dichiarato un errore di connessione.

Ad esempio, un valore pari a 1 in questo parametro indica che i messaggi devono essere ricevuti entro ogni intervallo RPI. Un valore 2 indica che 1 messaggio può andare perso se almeno 1 messaggio viene ricevuto nel giro di 2 intervalli RPI (2 x RPI).

Network Delay Multiplier

Il parametro Network Delay Multiplier definisce il tempo di trasferimento del messaggio applicato dal protocollo CIP Safety. Il valore di Network Delay Multiplier specifica il ritardo del percorso produttore-consumatore e del ritorno della conferma al produttore. È possibile utilizzare questo parametro per ridurre o aumentare il limite del tempo di risposta della connessione nei casi in cui il tempo di trasferimento del messaggio applicato è notevolmente inferiore o superiore all'intervallo RPI. Ad esempio, la regolazione di Network Delay Multiplier può essere utile quando l'RPI di una connessione di uscita corrisponde alla durata dell'intervallo del task di sicurezza.

Nei casi in cui l'intervallo RPI in ingresso o uscita è relativamente lento o veloce rispetto al ritardo del messaggio applicato, il valore di Network Delay Multiplier può essere approssimato utilizzando uno dei due metodi riportati di seguito.

Metodo 1: utilizzare il rapporto tra l'intervallo RPI degli ingressi e il periodo del task di sicurezza. È possibile utilizzare questo metodo solo se si verificano tutte le seguenti condizioni:

- Il percorso o il ritardo è quasi uguale al percorso o al ritardo di uscita.
- L'intervallo RPI degli ingressi è stato configurato in modo che il tempo di trasferimento effettivo del messaggio di ingresso sia inferiore a quello dell'intervallo RPI degli ingressi.
- Il periodo del task di sicurezza è lento rispetto all'intervallo RPI degli ingressi.

  In queste condizioni, il valore di Output Network Delay Multiplier può essere approssimato come segue:

  Moltiplicatore ritardo rete in ingresso x [RPI degli ingressi ÷ Periodo del task di sicurezza]

ESEMPIO	**Calcolo approssimativo del moltiplicatore ritardo rete in uscita**
	Se:
	RPI degli ingressi = 10 ms Moltiplicatore ritardo rete in ingresso = 200% Periodo del task di sicurezza = 20 ms
	Pertanto, il moltiplicatore ritardo rete in uscita equivale a:
	200% x [10 ÷ 20] = 100%

Metodo 2: utilizzare il ritardo di rete massimo osservato. Se il sistema funziona per un periodo prolungato nelle peggiori condizioni di carico, il moltiplicatore ritardo rete può essere impostato da ritardo rete massimo osservato. Questo metodo può essere utilizzato su una connessione di ingresso o uscita. Dopo che il sistema ha funzionato per un periodo di tempo prolungato nelle condizioni di carico peggiori, annotare il ritardo rete massimo osservato.

Il moltiplicatore ritardo rete può essere approssimato tramite la seguente equazione:

[Ritardo rete massimo osservato + Fattore_margine] ÷ RPI

ESEMPIO	**Calcolo del moltiplicatore ritardo rete da ritardo rete massimo osservato**
	Se:
	RPI = 50 ms Ritardo rete massimo osservato = 20 ms Fattore_margine = 10
	Pertanto, il moltiplicatore ritardo rete equivale a:
	[20 + 10] ÷ 50 = 60%

Tabella 18 - Ulteriori informazioni

Risorsa	Descrizione
GuardLogix 5570 Controllers Systems Safety Reference Manual, pubblicazione 1756-RM099	Fornisce informazioni sul calcolo dei tempi di risposta.
Manuale dell'utente Moduli di sicurezza Guard I/O DeviceNet, pubblicazione 1791DS-UM001J-IT-P	
Guard I/O EtherNet/IP Safety Modules User Manual, pubblicazione 1791ES-UM001	

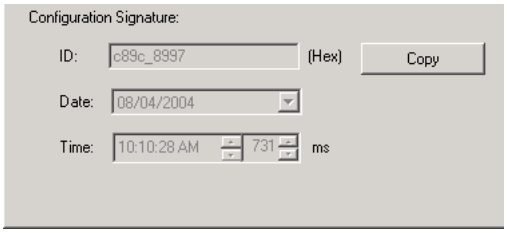
Comprensione dell'autenticazione di configurazione

Ogni dispositivo di sicurezza ha un'autenticazione di configurazione univoca, che definisce la configurazione del modulo. L'autenticazione di configurazione è composta da un numero ID, data e ora ed è utilizzata per verificare la configurazione di un modulo.

Configurazione mediante l'applicazione Logix Designer

Quando il dispositivo I/O viene configurato utilizzando l'applicazione Logix Designer, l'autenticazione di configurazione viene generata automaticamente. È possibile visualizzare e copiare l'autenticazione di configurazione tramite la scheda Safety nella finestra di dialogo Module Properties.

Figura 22 – Visualizzazione e copia dell'autenticazione di configurazione



Proprietario della configurazione diverso (connessione di solo ascolto)

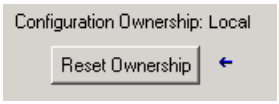
Se la configurazione del dispositivo I/O appartiene ad un altro controllore, occorre copiare l'autenticazione di configurazione del modulo dal progetto del proprietario e incollarla nella scheda Safety della finestra di dialogo Module Properties.

SUGGERIMENTO Se il dispositivo è configurato solo per gli ingressi, è possibile copiare e incollare l'autenticazione di configurazione. Se il dispositivo è dotato di uscite di sicurezza, queste appartengono al controllore proprietario della configurazione, pertanto la casella di testo dell'autenticazione di configurazione non è disponibile.

Ripristino della proprietà dei dispositivi I/O di sicurezza

Quando il progetto del controllore è online, nella scheda Safety della finestra di dialogo Module Properties viene visualizzata la proprietà di configurazione corrente. Quando la configurazione appartiene al progetto aperto, viene visualizzato "Local". Quando la configurazione appartiene ad un secondo dispositivo, viene visualizzato "Remote" insieme al numero rete di sicurezza (SNN) e all'indirizzo di nodo o al numero di slot del proprietario della configurazione. Se la lettura del dispositivo non riesce, viene visualizzato un errore di comunicazione.

Se il dispositivo è online, fare clic su Reset Ownership per riportare il dispositivo alla sua configurazione di fabbrica.



SUGGERIMENTO In presenza di modifiche in sospeso delle proprietà del modulo, una firma del task di sicurezza oppure un blocco di sicurezza, non è possibile ripristinare la proprietà.

Indirizzamento dei dati I/O di sicurezza

Quando si aggiunge un dispositivo alla cartella di configurazione I/O, per tale dispositivo l'applicazione Logix Designer crea automaticamente dei tag definiti nell'ambito del controllore.

Le informazioni I/O vengono presentate come set di tag. Ciascun tag utilizza una struttura di dati, a seconda del tipo e delle funzioni del dispositivo I/O. Il nome di un tag è basato sul nome del dispositivo utilizzato nel sistema.

Formato dell'indirizzo dei moduli I/O di sicurezza

Il formato degli indirizzi dei moduli I/O di sicurezza deve rispettare il seguente schema.

ESEMPIO Modulename:Type.Member

Tabella 19 - Formato degli indirizzi dei dispositivi I/O di sicurezza

Dove	È	
Modulename	Il nome del dispositivo I/O di sicurezza	
Type	Il tipo di dati	Ingresso: I Uscita: O
Member	Dati specifici dal dispositivo I/O	
	Modulo di solo ingresso	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Modulo di sola uscita	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	I/O misti	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Formato di indirizzo per i servoazionamenti Kinetix 5500 e Kinetix 5700 e per PowerFlex 527

Il formato degli indirizzi dei servoazionamenti Kinetix 5500 e Kinetix 5700 e di PowerFlex 527 deve rispettare il seguente schema.

ESEMPIO Drivename:Type.Member

Tabella 20 - Formato degli indirizzi dei dispositivi I/O di sicurezza per i servoazionamenti

Dove	È	
Drivename	Il nome del servoazionamento Kinetix o del convertitore PowerFlex	
Type	Il tipo di dati	Ingresso: SI Uscita: SO
Member	Dati specifici dal dispositivo I/O	
	Modulo di solo ingresso	Drivename:SI.ConnectionStatus Drivename:SI.RunMode Drivename:SI.ConnectionFaulted Drivename:SI.Status Drivename:SI.TorqueDisabled Drivename:SI.SafetyFault Drivename:SI.ResetRequired
	Modulo di sola uscita	Drivename:SO.Command Drivename:SO.SafeTorqueOff Drivename:SO.Reset

Tabella 21 - Altre risorse

Risorsa	Descrizione
Capitolo 9, Monitoraggio dello stato e gestione degli errori	Contiene informazioni sul monitoraggio dei dati dei tag di sicurezza
Dati I/O e tag dei controllori Logix5000 Manuale di programmazione, pubblicazione 1756-PM004C-IT-P	Fornisce informazioni sull'indirizzamento dei dispositivi I/O standard

Monitoraggio dello stato dei dispositivi I/O di sicurezza

Lo stato dei dispositivi I/O di sicurezza può essere monitorato per mezzo di messaggi espliciti o tramite gli indicatori di stato dei dispositivi I/O. Per informazioni sulla risoluzione dei problemi del modulo I/O, consultare i manuali dei prodotti Guard I/O elencati in Per ulteriori informazioni a pagina 11.

Tabella 22 - Funzionamento dell'indicatore di stato dei moduli Guard I/O

Indicatore	Stato	Descrizione		
		Moduli Guard I/O DeviceNet	**Moduli Guard I/O EtherNet/IP**	**Moduli POINT Guard I/O**
Stato del modulo (MS)	Spento	Alimentazione assente.		
	Verde, acceso fisso	Funzionamento normale.		
	Verde, lampeggiante	Dispositivo in stato di riposo.		
	Rosso, lampeggiante	Errore reversibile.	Si è verificato un errore reversibile oppure è in corso un aggiornamento del firmware.	
	Rosso, acceso	Errore irreversibile.		
	Rosso/verde, lampeggiante	Autodiagnosi in corso.	È in corso la procedura di autodiagnosi oppure il modulo non è configurato correttamente. Per ulteriori informazioni, fare riferimento all'indicatore di stato della rete.	
Stato della rete (NS)	Spento	Dispositivo non in linea o non alimentato.		
	Verde, acceso fisso	Dispositivo in linea, connessioni stabilite.		
	Verde, lampeggiante	Dispositivo in linea, nessuna connessione stabilita.		
	Rosso, lampeggiante	Timeout della comunicazione.	Si è verificato un timeout della comunicazione oppure è in corso un aggiornamento del firmware.	
	Rosso, acceso	Errore di comunicazione. Il dispositivo ha rilevato un errore che ha impedito la comunicazione di rete.		
	Rosso/verde, lampeggiante	Dispositivo nello stato di errore di comunicazione o impostazione del numero rete di sicurezza (SNN) in corso.	Autodiagnosi in corso.	Non applicabile.
Punti di ingresso (IN*x*)	Spento	Ingresso di sicurezza OFF.		
	Giallo, acceso	Ingresso di sicurezza ON.		
	Rosso, acceso	Errore nel circuito di ingresso.		
	Rosso, lampeggiante	Se è stato selezionato il funzionamento a doppio canale, si è verificato un errore nel circuito di ingresso associato.		
Punti di uscita (O*x*)	Spento	Uscita di sicurezza OFF.		
	Giallo, acceso	Uscita di sicurezza ON.		
	Rosso, acceso	Errore nel circuito di uscita.		
	Rosso, lampeggiante	Se è stato selezionato il funzionamento a doppio canale, si è verificato un errore nel circuito di uscita associato.		
Test punti di uscita (T*x*)	Spento	Non applicabile.	Uscita OFF.	Non applicabile.
	Giallo, acceso		Uscita ON.	
	Rosso, acceso		Errore nel circuito di uscita.	
LOCK (blocco)	Giallo, acceso	Configurazione del dispositivo bloccata.	L'applicazione Logix Designer non supporta questa funzione.	
	Giallo, lampeggiante	Configurazione del dispositivo valida, ma il dispositivo non è bloccato.		
	Giallo, spento	Dati di configurazione assenti o non validi o dispositivo configurato.		
IN PWR (alimentazione ingresso)	Verde, spento	Alimentazione ingresso assente.		Non applicabile.
	Verde, acceso fisso	La tensione di alimentazione di ingresso è conforme alle specifiche.		
	Giallo, acceso	La tensione di alimentazione di ingresso non è conforme alle specifiche.		
OUT PWR (alimentazione uscita)	Verde, spento	Alimentazione uscita assente.		
	Verde, acceso fisso	La tensione di alimentazione di uscita è conforme alle specifiche.		
	Giallo, acceso	La tensione di alimentazione di uscita non è conforme alle specifiche.		
PWR	Verde, spento	Non applicabile.		Alimentazione assente.
	Verde, acceso fisso			La tensione di alimentazione è conforme alle specifiche.
	Giallo, acceso			La tensione di alimentazione non è conforme alle specifiche.

Vedere pagina 11 per ulteriori informazioni sugli indicatori di stato per Kinetix 5500, Kinetix 5700 e PowerFlex 527.

Reset di un modulo alle condizioni predefinite in fabbrica

Se il modulo Guard I/O era già stato utilizzato in precedenza, cancellare la configurazione preesistente prima di installarlo su una rete di sicurezza ripristinandolo alle condizioni predefinite in fabbrica.

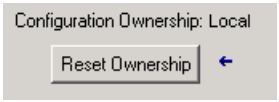
Quando il progetto del controllore è online, nella scheda Safety della finestra di dialogo Module Properties viene visualizzata la proprietà della configurazione corrente. Quando la configurazione appartiene al progetto aperto, viene visualizzato "Local". Quando la configurazione appartiene ad un secondo dispositivo, viene visualizzato "Remote" insieme al numero rete di sicurezza (SNN) e all'indirizzo di nodo o al numero di slot del proprietario della configurazione. Se la lettura del modulo non riesce, viene visualizzato un errore di comunicazione.

Se la connessione è Local, è necessario inibire la connessione del modulo prima del reset della proprietà. Per inibire il modulo, procedere come segue.

1. Fare clic con il pulsante destro del mouse sul modulo e selezionare Properties.
2. Fare clic sulla scheda Connection.
3. Selezionare Inhibit Connection.
4. Fare clic su Apply e quindi su OK.

Per ril reset del modulo alla configurazione predefinita in fabbrica in modalità online, procedere come segue.

1. Fare clic con il pulsante destro del mouse sul modulo e selezionare Properties.
2. Fare clic sulla scheda Safety.
3. Fare clic su Reset Ownership.



Sostituzione di un dispositivo utilizzando l'applicazione Logix Designer

Per sostituire un dispositivo I/O di sicurezza su una rete Ethernet, è possibile usare l'applicazione Logix Designer. Per sostituire un modulo Guard I/O su una rete DeviceNet, la scelta dipende dal tipo di modulo.

Tabella 23 - Software

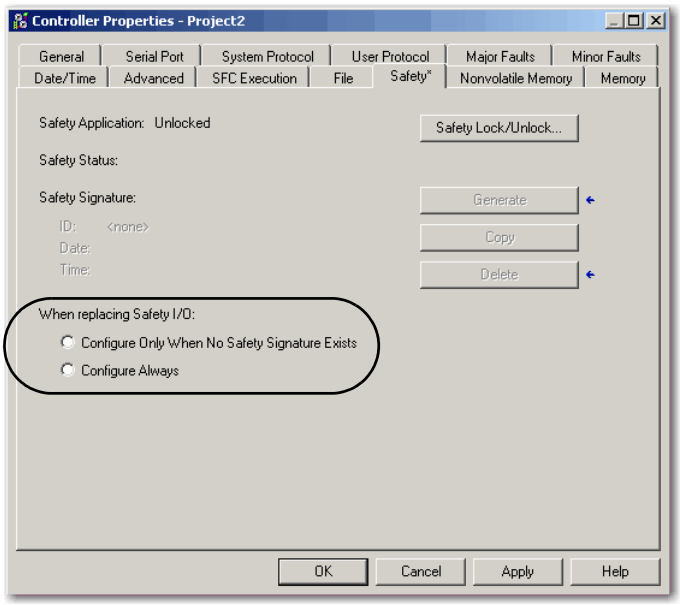
Se si utilizza	Usare	Vedere
Modulo Guard I/O 1791DS con adattatore 1756-DNB	Applicazione Logix Designer	Sotto
Modulo POINT Guard I/O 1734 con adattatore 1734-PDN	Software RSNetWorx for DeviceNet	Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet a pagina 81

Se si sta utilizzando una parte del sistema CIP safety per garantire la conformità al livello SIL 3 durante la sostituzione e il test funzionale del dispositivo, non è possibile utilizzare la funzione Configure Always. Consultare Sostituzione con l'opzione "Configure Only When No Safety Signature Exists" abilitata a pagina 76.

Se non si utilizza l'intero sistema di controllo CIP safety instradabile per garantire la conformità con il livello SIL 3/PLe durante la sostituzione e il test funzionale di un dispositivo, è possibile utilizzare la funzione Configure Always. Consultare Sostituzione con l'opzione "Configure Always" abilitata a pagina 80.

La sostituzione del dispositivo I/O di sicurezza si configura sulla scheda Safety del controllore GuardLogix.

Figura 23 – Sostituzione dei dispositivi I/O di sicurezza



Sostituzione con l'opzione "Configure Only When No Safety Signature Exists" abilitata

Quando viene sostituito un dispositivo I/O di sicurezza, se il DeviceID del nuovo dispositivo corrisponde all'originale, la configurazione viene scaricata dal controllore di sicurezza. Il DeviceID è una combinazione dell'indirizzo di nodo/IP e del numero di rete di sicurezza (SNN) e viene aggiornato ogni volta che viene impostato il numero SNN.

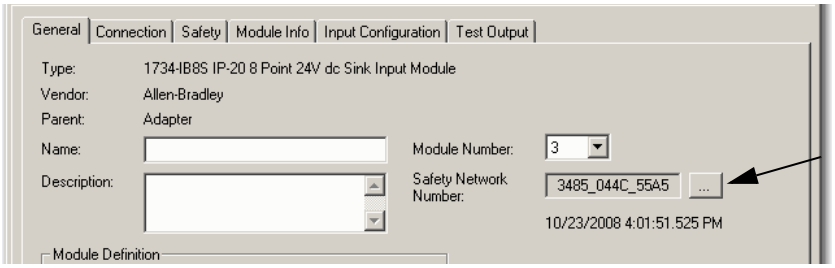
Se il progetto è configurato come "Configure Only When No Safety Signature Exists", fare riferimento ai punti corrispondenti nella Tabella 24 per sostituire un dispositivo I/O di sicurezza in base allo scenario effettivo. Una volta completata correttamente la procedura, il DeviceID corrisponde all'originale e consente al controllore di sicurezza di scaricare la corretta configurazione del dispositivo e di ristabilire la connessione di sicurezza.

Tabella 24 - Sostituzione di un modulo

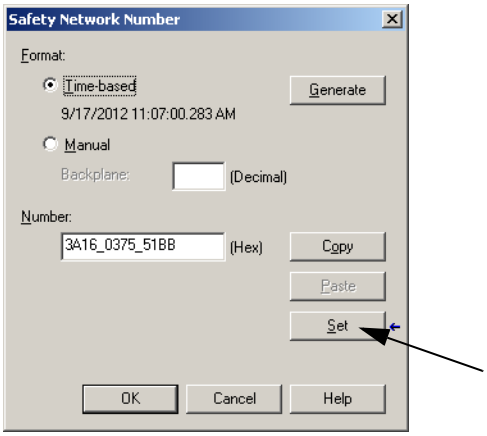
Con firma di sicurezza GuardLogix	Condizione modulo sostitutivo	Intervento necessario
No	Senza SNN (originale)	Nessuna. Il dispositivo è pronto all'uso.
Sì o No	Stesso SNN della configurazione task di sicurezza originale	Nessuna. Il dispositivo è pronto all'uso.
Sì	Senza SNN (originale)	Vedere Scenario 1 – Dispositivo sostitutivo nelle condizioni predefinite in fabbrica e presenza della firma di sicurezza a pagina 77.
Sì	SNN differente dalla configurazione task di sicurezza originale	Vedere Scenario 2 – Numero SNN del dispositivo sostitutivo diverso dall'originale e presenza della firma di sicurezza a pagina 78.
No		Vedere Scenario 3 – Numero SNN del dispositivo sostitutivo diverso dall'originale e assenza della firma di sicurezza a pagina 79.

Scenario 1 – Dispositivo sostitutivo nelle condizioni predefinite in fabbrica e presenza della firma di sicurezza

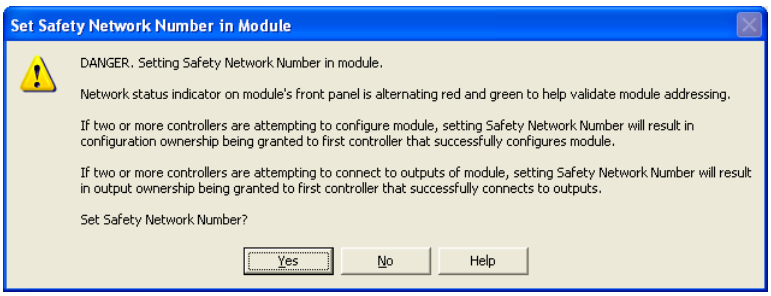
1. Rimuovere il dispositivo I/O in uso e installare quello nuovo.
2. Fare clic con il pulsante destro del mouse sul dispositivo I/O di sicurezza sostitutivo e selezionare Properties.
3. Per aprire la finestra di dialogo Safety Network Number, fare clic su ... a destra del numero rete di sicurezza.



4. Fare clic su Set.



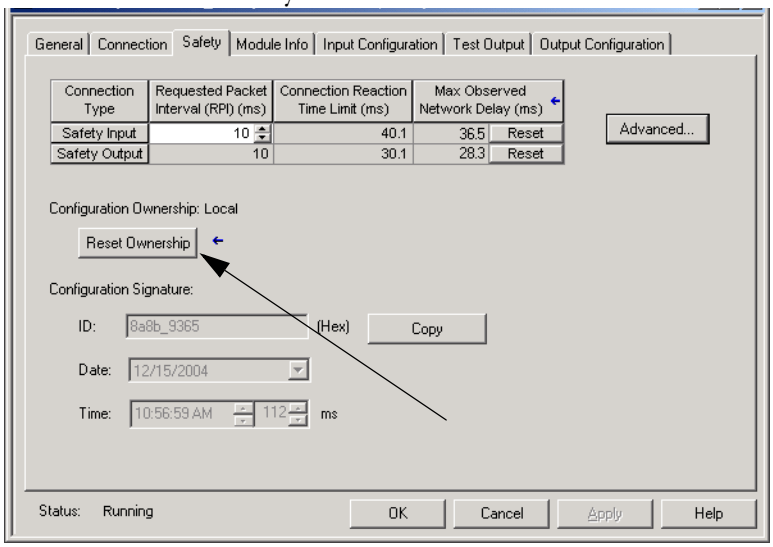
5. Verificare che l'indicatore di stato della rete (NS) lampeggi con luce alternata rossa/verde sul dispositivo corretto prima di fare clic su Yes nella finestra di dialogo di conferma per impostare l'SNN e accettare il dispositivo sostitutivo.



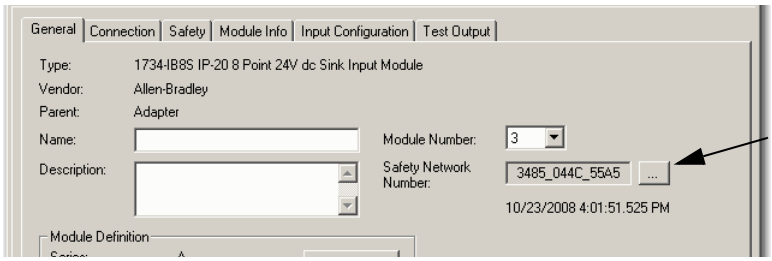
6. Seguire le procedure indicate dalla propria società per il test funzionale del dispositivo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

Scenario 2 – Numero SNN del dispositivo sostitutivo diverso dall'originale e presenza della firma di sicurezza

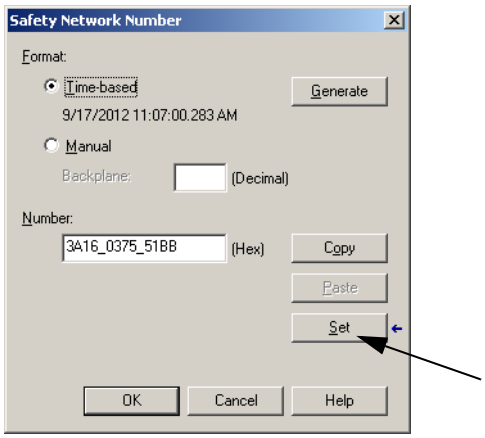
1. Rimuovere il dispositivo I/O in uso e installare quello nuovo.
2. Fare clic con il pulsante destro del mouse sul proprio dispositivo I/O di sicurezza e selezionare Properties.
3. Fare clic sulla scheda Safety.



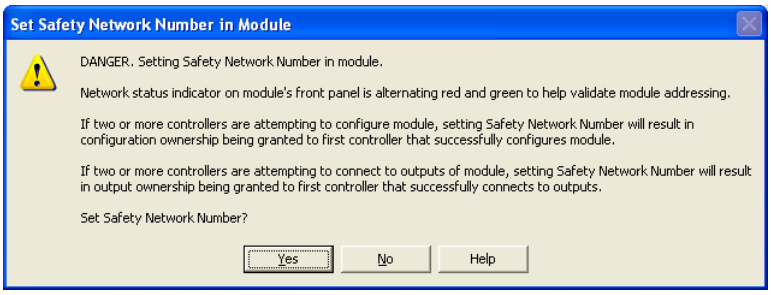
4. Fare clic su Reset Ownership.
5. Fare clic su OK.
6. Fare clic con il pulsante destro del mouse sul dispositivo e selezionare Properties.
7. Per aprire la finestra di dialogo Safety Network Number, fare clic su ... a destra del numero rete di sicurezza.



8. Fare clic su Set.



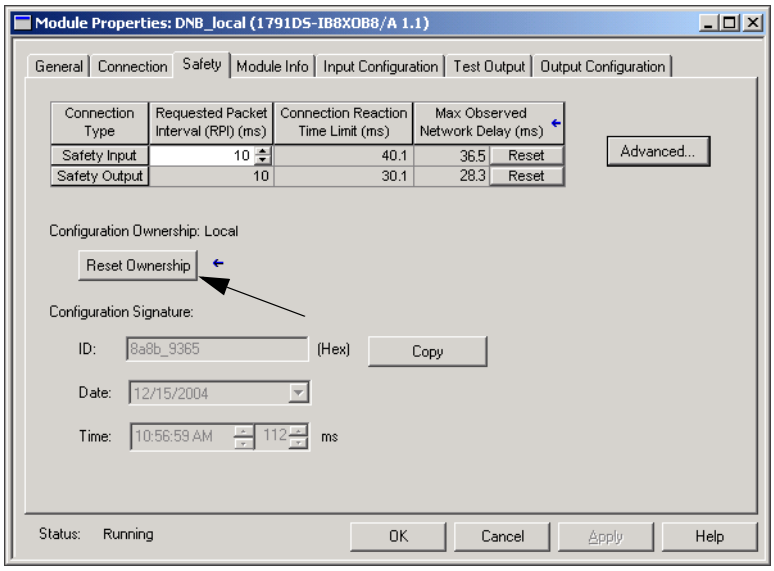
9. Verificare che l'indicatore di stato della rete (NS) lampeggi con luce alternata rossa/verde sul dispositivo corretto prima di fare clic su Yes nella finestra di dialogo di conferma per impostare l'SNN e accettare il dispositivo sostitutivo.



10. Seguire le procedure indicate dalla propria società per il test funzionale del dispositivo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

Scenario 3 – Numero SNN del dispositivo sostitutivo diverso dall'originale e assenza della firma di sicurezza

1. Rimuovere il dispositivo I/O in uso e installare quello nuovo.
2. Fare clic con il pulsante destro del mouse sul proprio dispositivo I/O di sicurezza e selezionare Properties.
3. Fare clic sulla scheda Safety.



4. Fare clic su Reset Ownership.
5. Fare clic su OK.
6. Seguire le procedure indicate dalla propria società per il test funzionale del dispositivo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

Sostituzione con l'opzione "Configure Always" abilitata

ATTENZIONE: Abilitare la funzione "Configure Always" solo se l'intero sistema di controllo CIP Safety **non** è utilizzato per mantenere il livello SIL 3 durante la sostituzione e il test funzionale di un dispositivo.

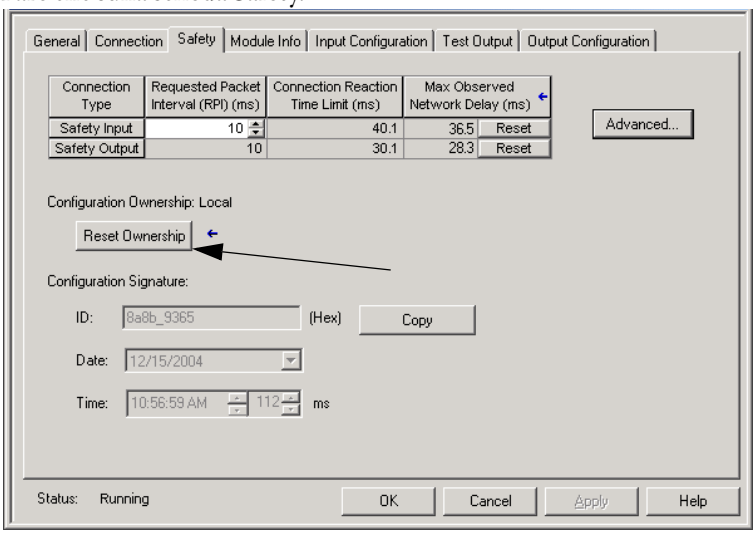
Non posizionare i dispositivi impostati su valori predefiniti di fabbrica su una rete di sicurezza CIP con la funzione Configure Always abilitata, a meno che non si stia seguendo la presente procedura di sostituzione.

Se nel progetto del controllore la funzione "Configure Always" è abilitata, il controllore verifica e collega automaticamente un dispositivo sostitutivo che soddisfi tutti i seguenti requisiti:

- Il controllore dispone di dati di configurazione per un dispositivo compatibile all'indirizzo di rete specificato.
- Il dispositivo è nelle condizioni predefinite in fabbrica o ha un numero SNN che corrisponde alla configurazione.

Se il progetto è configurato per "Configure Always", seguire la procedura adeguata per sostituire un dispositivo I/O di sicurezza.

1. Rimuovere il dispositivo I/O in uso e installare quello nuovo.
   a. Se il dispositivo è nelle condizioni predefinite in fabbrica, andare al punto 6.
   Non è necessaria alcuna azione da parte del controllore GuardLogix per assumere la proprietà del dispositivo.
   b. In caso di errore di mancata corrispondenza del numero SNN, andare al punto successivo per ripristinare il dispositivo alle condizioni predefinite in fabbrica.
2. Fare clic con il pulsante destro del mouse sul proprio dispositivo I/O di sicurezza e selezionare Properties.
3. Fare clic sulla scheda Safety.



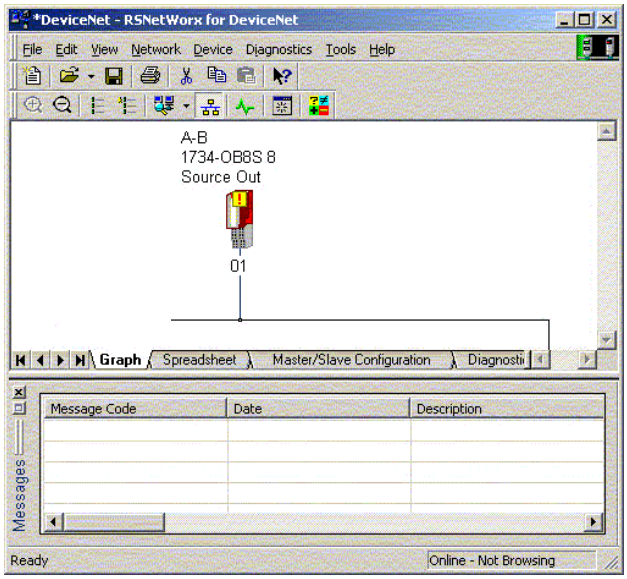
4. Fare clic su Reset Ownership.
5. Fare clic su OK.
6. Seguire le procedure indicate dalla propria società per il test funzionale del dispositivo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

Sostituzione di un modulo POINT Guard I/O mediante il software RSNetWorx for DeviceNet

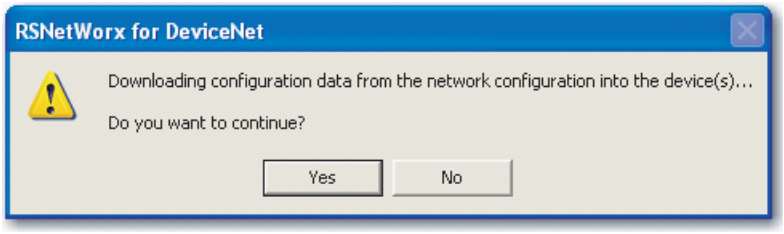
Per sostituire un modulo POINT Guard I/O quando modulo e controllore si trovano in una rete DeviceNet, procedere come segue.

1. Sostituire il modulo e far corrispondere il numero di nodo del modulo originale.
2. Nel software RSNetWorx for DeviceNet, aprire il progetto.

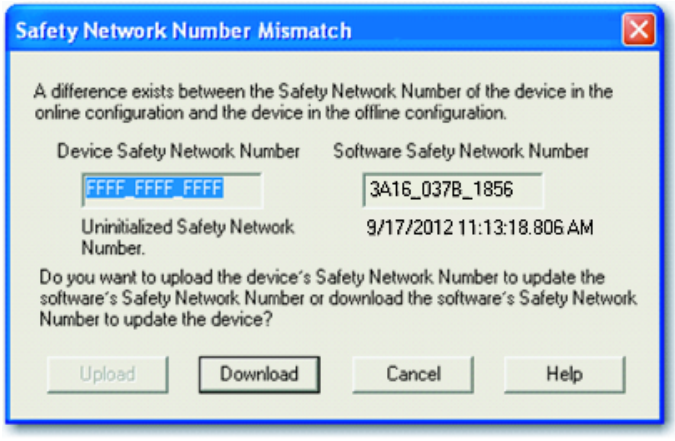
   Se è nuovo o ha un numero SNN che non corrisponde a quello del modulo originale, il modulo sostitutivo viene visualizzato con un punto esclamativo.



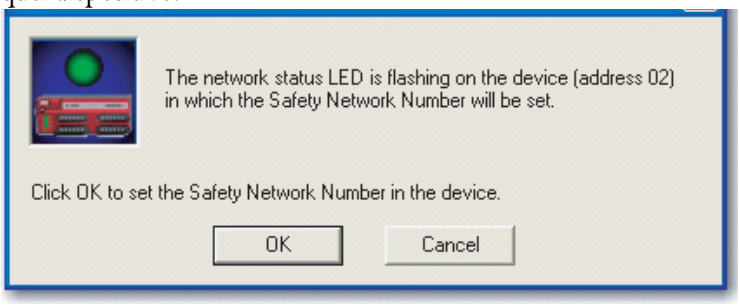
3. Fare clic con il pulsante destro del mouse sul modulo e selezionare Download to Device.



4. Fare clic su Yes per confermare.
5. Fare clic su Download nella finestra di dialogo Safety Network Number Mismatch per impostare il numero SNN sul modulo sostitutivo.

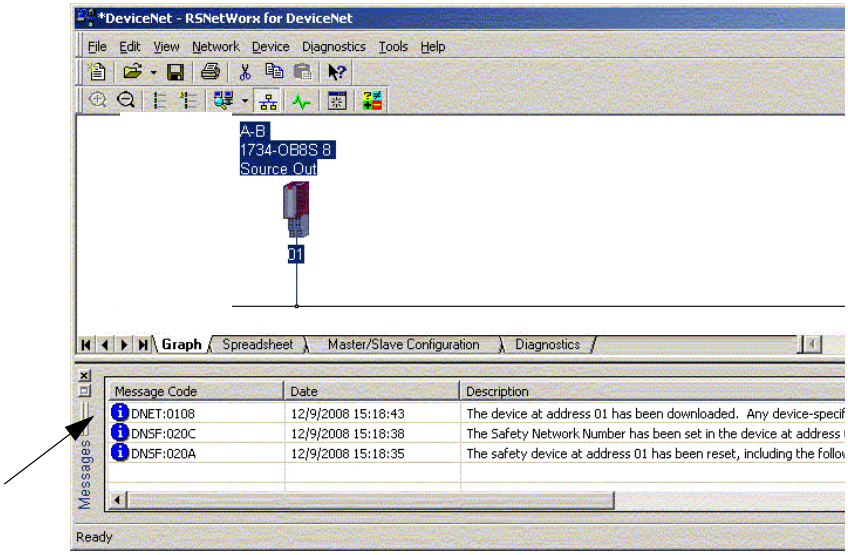


6. Verificare che l'indicatore dello stato della rete (NS) lampeggi sul modulo corretto e fare clic su OK per impostare il numero SNN su quel dispositivo.



Il software RSNetWorx for DeviceNet conferma che il numero SNN è stato impostato.

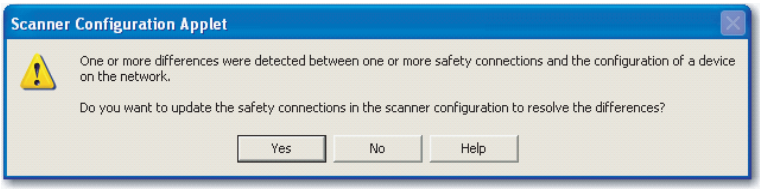
Una volta completato e riuscito il download, la vista del progetto principale visualizza questo messaggio: "The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately."



Presumendo che questa sia la configurazione corretta acquisita dal file DNT originale, il numero SNN e l'autenticazione di configurazione ora corrispondono all'originale. Se il controllore è già collegato, viene stabilita una connessione. Il controllore non ha bisogno di uscire dalla modalità Esecuzione per il download nel modulo sostitutivo.

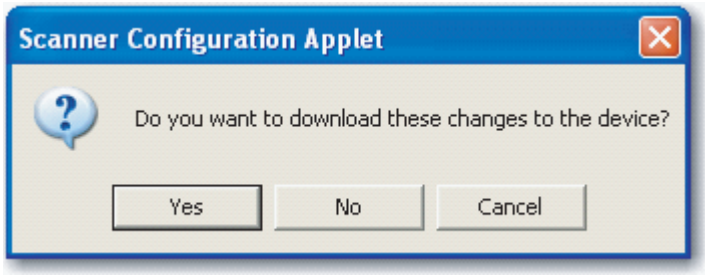
Se si scarica questa configurazione per uso temporaneo, inserire il modulo nella rete ed esso si collega automaticamente al controllore.

Se la configurazione scaricata nel modulo non proviene dal file DNT originale, l'autenticazione di configurazione non corrisponderà all'originale. Anche se si ricreano gli stessi parametri in un nuovo file DNT, le parti relative ad ora e data dell'autenticazione saranno diverse e la connessione al controllore non avviene. In tal caso, fare clic sulla scheda Safety Connection del controllore che ha segnalato la diversa autenticazione di configurazione e che offre la possibilità di far corrispondere la nuova autenticazione di configurazione. Tuttavia, convalidare nuovamente il sistema di sicurezza perché non sta usando il file DNT originale.



7. Fare clic su Yes.

   Questa azione interrompe la modalità Esecuzione del controllore e invita a scaricare le modifiche.



8. Fare clic su Yes per scaricare la nuova configurazione di connessione nel controllore.

   Al termine del download, riportare il controllore in modalità Esecuzione e la connessione al modulo sostitutivo viene stabilita.

9. Seguire le procedure indicate dalla propria società per il test funzionale del modulo I/O sostituito e del sistema nonché per autorizzare l'uso del sistema.

Note:

Sviluppo di applicazioni di sicurezza

Argomento	Pagina
Task di sicurezza	86
Programmi di sicurezza	87
Routine di sicurezza	88
Tag di sicurezza	88
Tag di sicurezza prodotti/consumati	92
Mappatura dei tag di sicurezza	98
Protezione dell'applicazione di sicurezza	100
Programmazione delle restrizioni	103

In questo capitolo vengono descritti i componenti di un progetto di sicurezza e vengono fornite informazioni relative all'utilizzo delle funzioni che contribuiscono a proteggere l'integrità dell'applicazione di sicurezza, come la firma del task di sicurezza e il blocco di sicurezza.

Per le regole generali e i requisiti relativi allo sviluppo e alla messa in servizio di applicazioni di sicurezza SIL 3 e PLe, consultare il Manuale di riferimento per la sicurezza Sistemi di controllo GuardLogix 5570, pubblicazione 1756-RM099B-IT-P.

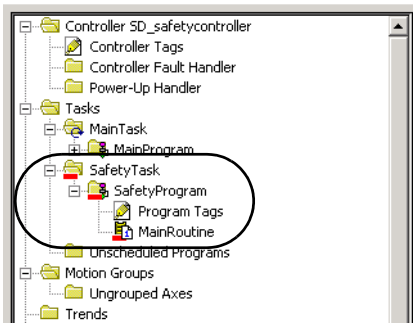
In questo manuale di riferimento per la sicurezza vengono trattati i seguenti argomenti:

- Creazione di una specifica dettagliata del progetto
- Sviluppo, documentazione e collaudo dell'applicazione
- Generazione della firma del task di sicurezza per l'identificazione e la protezione del progetto
- Conferma del progetto mediante la stampa o la visualizzazione del progetto caricato e confronto manuale delle configurazioni, dei dati di sicurezza e della logica del programma di sicurezza
- Verifica del progetto tramite casi di test, simulazioni, test di verifica funzionale e, se richiesto, una verifica di sicurezza indipendente
- Blocco dell'applicazione di sicurezza
- Calcolo del tempo di risposta del sistema

Task di sicurezza

Quando viene creato un progetto del controllore di sicurezza, l'applicazione Logix Designer genera automaticamente un task di sicurezza con un programma di sicurezza e una routine (di sicurezza) principale.

Figura 24 – Task di sicurezza nell'organizer del controllore



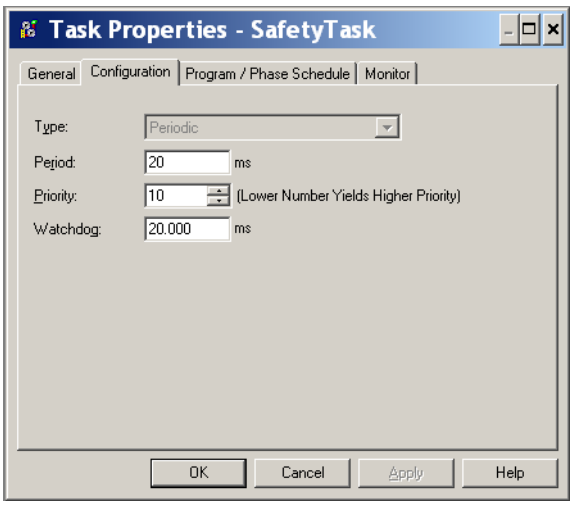
All'interno del task di sicurezza, è possibile utilizzare diversi programmi di sicurezza, costituiti da più routine di sicurezza. Il controllore GuardLogix supporta un task di sicurezza. Il task di sicurezza non può essere eliminato.

Inoltre, non è possibile schedulare programmi standard o eseguire routine standard all'interno del task di sicurezza.

Definizione del periodo del task di sicurezza

Il task di sicurezza è un task periodico. La priorità del task e il tempo del watchdog vengono specificati nella finestra di dialogo Task Properties – Safety Task. Per aprire la finestra di dialogo, fare clic con il pulsante destro del mouse sul task di sicurezza e selezionare Properties.

Figura 25 – Configurazione del periodo del task di sicurezza



Il task di sicurezza ha una priorità elevata. È necessario specificare il periodo e il watchdog del task di sicurezza (entrambi in ms). Il periodo del task di sicurezza è il periodo in cui viene eseguito il task di sicurezza. Il watchdog del task di sicurezza è il tempo massimo consentito per l'esecuzione del task, dall'avvio fino al completamento.

Il periodo del task di sicurezza è limitato ad un massimo di 500 ms e non può essere modificato in modalità online. Accertarsi che il task di sicurezza possa completare l'esecuzione logica prima dell'attivazione successiva. Se si verifica un timeout del watchdog del task di sicurezza, viene generato un errore di sicurezza irreversibile nel controllore di sicurezza.

Il periodo del task di sicurezza influisce direttamente sul tempo di risposta del sistema.

Il Manuale di riferimento per la sicurezza - Sistemi di controllo GuardLogix 5570, pubblicazione 1756-RM099B-IT-P, contiene informazioni dettagliate sul calcolo del tempo di risposta del sistema.

Esecuzione del task di sicurezza

Il task di sicurezza viene eseguito allo stesso modo di un task periodico standard, con le seguenti eccezioni:

- L'esecuzione del task di sicurezza non inizia finché il controllore primario e il coprocessore di sicurezza non stabiliscono la partnership di controllo (i task standard, tuttavia, vengono eseguiti non appena il controllore passa in modalità Esecuzione).
- Tutti i tag di ingresso di sicurezza (immessi, consumati e mappati) vengono aggiornati e bloccati all'inizio dell'esecuzione del task di sicurezza.

  Per informazioni sulla mappatura dei tag di sicurezza, vedere a pagina 98.
- I valori dei tag di uscita di sicurezza (emessi e prodotti) vengono aggiornati alla conclusione dell'esecuzione del task di sicurezza.

Programmi di sicurezza

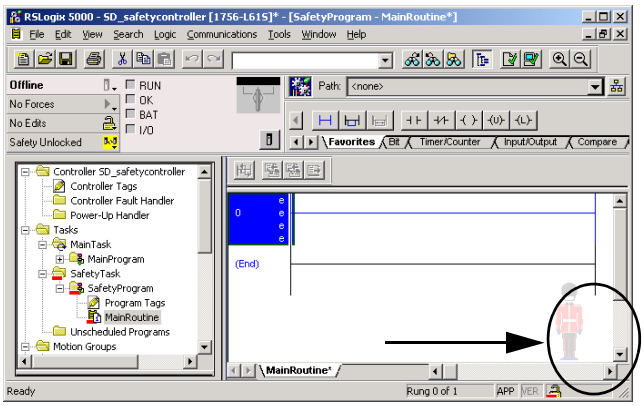
I programmi di sicurezza possiedono tutti gli attributi dei programmi standard, con l'eccezione che è possibile schedularli solo nel task di sicurezza e possono contenere solo componenti di sicurezza. I programmi di sicurezza possono contenere soltanto delle routine di sicurezza. È necessario designare una routine di sicurezza come routine principale; è possibile designare un'altra routine di sicurezza come routine di errore.

I programmi di sicurezza non possono contenere routine o tag standard.

Routine di sicurezza

Le routine di sicurezza possiedono tutti gli attributi delle routine standard, ma possono esistere esclusivamente all'interno di un programma di sicurezza. Attualmente, per le routine di sicurezza è possibile utilizzare solo il linguaggio ladder.

SUGGERIMENTO Una routine di sicurezza si distingue visivamente da una routine standard per la presenza di una filigrana.



Tag di sicurezza

Un tag è l'area della memoria di un controllore in cui vengono memorizzati i dati. I tag rappresentano il meccanismo di base per l'allocazione della memoria, per la creazione di riferimenti dei dati per la logica e per il monitoraggio dei dati. I tag di sicurezza possiedono tutti gli attributi dei tag standard con l'aggiunta di meccanismi certificati per garantire l'integrità dei dati SIL 3.

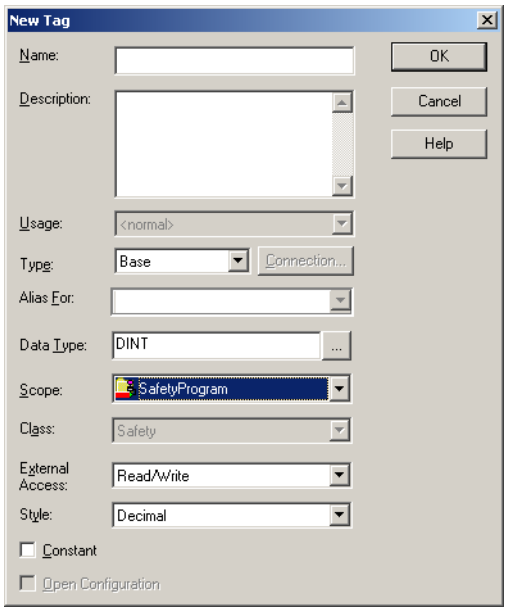
Al momento della creazione, al tag vengono assegnate le seguenti proprietà:

- Nome
- Descrizione (facoltativa)
- Tipo di tag
- Tipo di dati
- Ambito
- Classe
- Stile
- Accesso esterno

È inoltre possibile specificare se il valore del tag è costante.

Per creare un tag di sicurezza, aprire la finestra di dialogo New Tag facendo clic con il pulsante destro del mouse su Controller Tags o Program Tags e selezionare New Tag.

Figura 26 – Creazione di un nuovo tag



Tipo di tag

La Tabella 25 definisce i quattro possibili tipi di tag:

Tabella 25 – Quattro tipi di tag

Tipo di tag	Descrizione
Tag base	I tag di base memorizzano i valori che la logica deve utilizzare all'interno del progetto.
Tag alias	Un tag alias è un tag che fa riferimento ad un altro tag. Un tag alias può fare riferimento ad un altro tag alias o ad un tag base. Un tag alias può fare riferimento anche al componente di un altro tag, tramite il riferimento al membro di una struttura, all'elemento di una matrice o ad un bit incluso in un tag o in un membro. **IMPORTANTE:** non utilizzare i tag alias tra tag standard e di sicurezza all'interno delle applicazioni di sicurezza. Al contrario, i tag standard possono essere mappati ai tag di sicurezza mediante la mappatura dei tag di sicurezza. Vedere Mappatura dei tag di sicurezza a pagina 98.
Tag prodotto	Il tag prodotto è un tag del controllore che può essere utilizzato anche da altri controllori. I dati possono essere consumati (ricevuti) contemporaneamente da un massimo di 15 controllori. Un tag prodotto invia i propri dati ad uno o più tag consumatori senza usare la logica. I dati del tag prodotto vengono inviati in base all'intervallo RPI (Requested Packet Interval, intervallo di pacchetto richiesto) del tag consumatore.
Tag consumato	Un tag consumato è un tag che riceve i dati da un tag prodotto. Il tipo di dati del tag consumato deve corrispondere al tipo di dati del tag prodotto. L'intervallo di pacchetto richiesto (RPI) del tag consumato determina il periodo di aggiornamento dei dati.

Tipo di dati

Il tipo di dati permette di definire il tipo di dati memorizzati nel tag, ad esempio bit o numeri interi.

I tipi di dati possono essere combinati per formare delle strutture. Una struttura è caratterizzata da un tipo di dati univoco corrispondente ad un'esigenza specifica. All'interno di una struttura, ciascun tipo di dati viene definito membro. Analogamente ai tag, ai membri vengono associati un nome ed un tipo di dati. È possibile creare strutture personalizzate come tipi di dati definiti dall'utente.

I controllori Logix contengono tipi di dati predefiniti da utilizzare con istruzioni specifiche.

Per i tag di sicurezza sono ammessi i seguenti tipi di dati.

Tabella 26 – Tipi di dati validi per i tag di sicurezza

AUX_VALVE_CONTROL	DCI_STOP_TEST_MUTE	MANUAL_VALVE_CONTROL
BOOL	DINT	MUTING_FOUR_SENSOR_BIDIR
CAM_PROFILE	DIVERSE_INPUT	MUTING_TWO_SENSOR_ASYM
CAMSHAFT_MONITOR	EIGHT_POS_MODE_SELECTOR	MUTING_TWO_SENSOR_SYM
CB_CONTINUOUS_MODE	EMERGENCY_STOP	MOTION_INSTRUCTION
CB_CRANKSHAFT_POS_MONITOR	ENABLE_PENDANT	PHASE
CB_INCH_MODE	EXT_ROUTINE_CONTROL	PHASE_INSTRUCTION
CB_SINGLE_STROKE_MODE	EXT_ROUTINE_PARAMETERS	REDUNDANT_INPUT
CONFIGURABLE_ROUT	FBD_BIT_FIELD_DISTRIBUTE	REDUNDANT_OUTPUT
CONNECTION_STATUS	FBD_CONVERT	SAFETY_MAT
CONTROL	FBD_COUNTER	SERIAL_PORT_CONTROL
COUNTER	FBD_LOGICAL	SFC_ACTION
DCA_INPUT	FBD_MASK_EQUAL	SFC_STEP
DCAF_INPUT	FBD_MASKED_MOVE	SFC_STOP
DCI_MONITOR	FBD_TIMER	SINT
DCI_START	FIVE_POS_MODE_SELECTOR	STRING
DCI_STOP	INT	THRS_ENHANCED
DCI_STOP_TEST	LIGHT_CURTAIN	TIMER
DCI_STOP_TEST_LOCK	MAIN_VALVE_CONTROL	TWO_HAND_RUN_STATION

Ambito

L'ambito di un tag determina il punto in cui è possibile accedere ai dati del tag. Al momento della creazione, un tag viene definito come tag del controllore (dati globali) o tag del programma per un programma di sicurezza o standard specifico (dati locali). I tag di sicurezza possono essere definiti nell'ambito del controllore o del programma di sicurezza.

Tag definiti nell'ambito del controllore

Se i tag di sicurezza vengono inclusi nell'ambito del controllore, tutti i programmi possono accedere ai dati di sicurezza. I tag devono essere definiti nell'ambito del controllore se utilizzati nei seguenti casi:

- Per più programmi del progetto
- Per produrre o consumare dati
- Per la comunicazione con un terminale PanelView™
- Per la mappatura dei tag di sicurezza

  Per ulteriori informazioni, vedere Mappatura dei tag di sicurezza a pagina 98.

I tag di sicurezza definiti nell'ambito del controllore possono essere letti, ma non scritti, dalle routine standard.

IMPORTANTE	I tag di sicurezza nell'ambito del controllore possono essere letti da qualsiasi routine standard. La frequenza di aggiornamento dei tag di sicurezza si basa sul periodo del task di sicurezza.

I tag associati a I/O di sicurezza e a dati di sicurezza prodotti o consumati devono essere necessariamente tag di sicurezza definiti nell'ambito del controllore. Per i tag di sicurezza prodotti/consumati, è necessario creare un tipo di dati definito dall'utente e il primo membro della struttura di tag deve essere riservato allo stato della connessione. Tale membro è un tipo di dato predefinito denominato CONNECTION_STATUS.

Tabella 27 – Ulteriori risorse

Risorsa	Descrizione
Connessioni di sicurezza a pagina 121	Fornisce ulteriori informazioni sul membro CONNECTION_STATUS
Manuale di programmazione Dati I/O e tag dei controllori Logix5000, pubblicazione 1756-PM004C-IT-P	Fornisce istruzioni per la creazione di tipi di dati definiti dall'utente

Tag definiti nell'ambito del programma

Se i tag vengono definiti nell'ambito del programma, i dati non sono accessibili da altri programmi. Il riutilizzo di nomi di tag definiti nell'ambito di un programma è consentito in programmi diversi.

I tag di sicurezza definiti nell'ambito di un programma di sicurezza possono essere letti o scritti solo in una routine di sicurezza definita nell'ambito dello stesso programma di sicurezza.

Classe

I tag possono essere classificati come tag standard o di sicurezza. I tag classificati come tag di sicurezza devono avere un tipo di dati valido per i tag di sicurezza.

Quando vengono creati tag definiti nell'ambito di un programma, la classe viene specificata automaticamente a seconda che il tag sia stato creato in un programma standard o di sicurezza.

La classe dei tag creati nell'ambito del controllore, invece, deve essere specificata manualmente.

Valore costante

Quando un tag viene designato come valore costante, non può essere modificato dalla logica del controllore o da un'applicazione esterna come un pannello operatore. I tag con valori costanti non possono essere forzati.

L'applicazione Logix Designer può modificare i tag standard e di sicurezza con valori costanti, a patto che non sia presente una firma del task di sicurezza. I tag di sicurezza non possono essere modificati se è presente una firma del task di sicurezza.

Accesso esterno

Accesso esterno definisce il livello di accesso consentito per i dispositivi esterni, ad esempio un pannello operatore, per la visualizzazione o la modifica dei valori dei tag. L'accesso attraverso l'applicazione Logix Designer non è interessato da questa impostazione. Il valore predefinito è lettura/scrittura.

Tabella 28 – Livelli di accesso esterno

Impostazione di accesso esterno	Descrizione
Nessuna	I tag non sono accessibili dall'esterno del controllore.
Sola lettura	È possibile selezionare o leggere i tag, ma non scriverli dall'esterno del controllore.
Lettura/scrittura	È possibile selezionare o leggere i tag standard e scriverli dall'esterno del controllore.

Nel caso dei tag alias, il tipo di accesso esterno corrisponde al tipo configurato per il tag di destinazione base.

Tag di sicurezza prodotti/consumati

Per trasferire i dati di sicurezza tra controllori GuardLogix, si utilizzano tag di sicurezza prodotti e consumati. I tag prodotti e consumati richiedono connessioni. Il tipo di connessione di default per i tag prodotti e consumati è unicast.

Tabella 29 – Connessioni prodotte e consumate

Tag	Descrizione della connessione
Prodotto	Un controllore GuardLogix può produrre (inviare) tag di sicurezza verso altri controllori GuardLogix 1756 o 1768. Il controllore produttore utilizza un'unica connessione per ciascun consumatore.
Consumato	I controllori GuardLogix possono consumare (ricevere) tag di sicurezza da altri controllori GuardLogix 1756 o 1768. Ciascun tag consumato consuma una connessione.

I tag di sicurezza prodotti e consumati sono soggetti alle seguenti restrizioni:

- Solo i tag di sicurezza definiti nell'ambito controllore possono essere condivisi.
- La dimensione dei tag di sicurezza prodotti e consumati è limitata a 128 byte.
- Le coppie di tag prodotti/consumati devono essere dello stesso tipo di dati definito dall'utente.
- Il primo membro del tipo di dati definito dall'utente deve essere il tipo di dati predefinito CONNECTION_STATUS.
- L'intervallo di pacchetto richiesto (RPI, Requested Packet Interval) del tag di sicurezza consumato deve corrispondere al periodo del task di sicurezza del controllore GuardLogix produttore.

Per configurare correttamente i tag di sicurezza prodotti e consumati per la condivisione dei dati tra controllori di sicurezza peer, è necessario configurare correttamente i controllori di sicurezza peer, produrre un tag di sicurezza e consumare un tag di sicurezza, come descritto di seguito.

Configurazione dei numeri di rete di sicurezza dei controllori di sicurezza peer

Il controllore di sicurezza peer è soggetto agli stessi requisiti di configurazione del controllore di sicurezza locale. Il controllore di sicurezza peer deve inoltre essere dotato di un numero di rete di sicurezza (SNN). Il valore SNN del controllore di sicurezza peer varia in base al relativo posizionamento nel sistema.

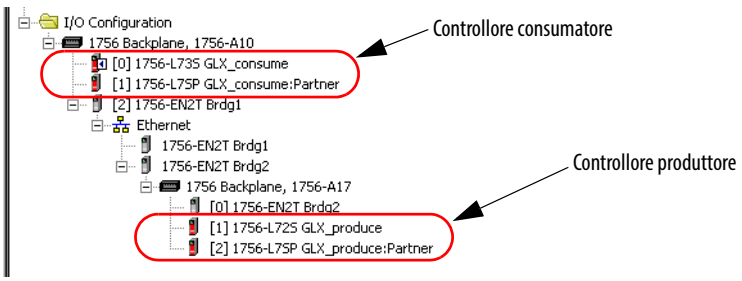
Tabella 30 – SNN e posizione del controllore

Posizione del controllore di sicurezza peer	SNN
Collocato nello chassis locale	I controllori GuardLogix nello stesso chassis hanno lo stesso SNN.
Collocato in un altro chassis	Il controllore deve avere un valore SNN univoco.

Per copiare e incollare il numero SNN, procedere come segue.

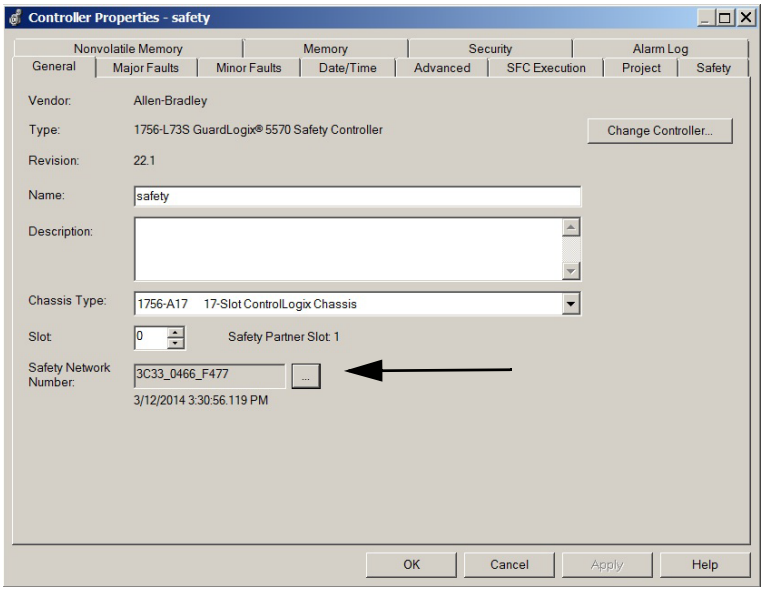
1. Aggiungere il controllore produttore all'albero I/O del controllore consumatore.

SUGGERIMENTO Uno stesso controllore produttore non può apparire più di una volta nell'albero I/O del controllore; in caso contrario viene generato un errore.

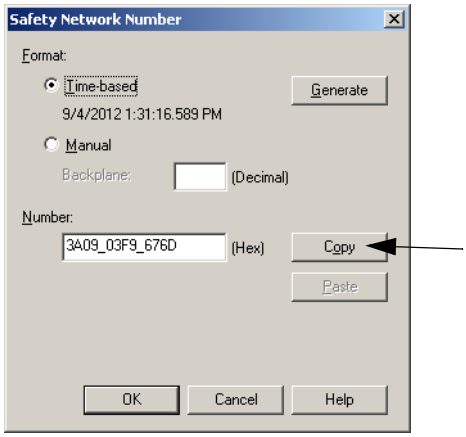


2. Nel progetto del controllore produttore, fare clic con il pulsante destro del mouse sul controllore produttore e selezionare Controller Properties.

3. Fare clic su ... per aprire la finestra di dialogo Safety Network Number.



4. Copiare il numero SNN del controllore produttore.



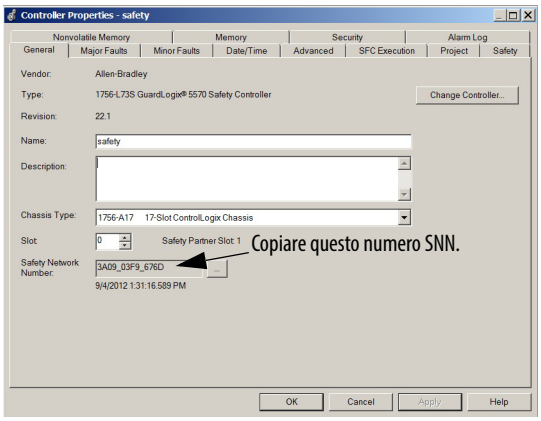
5. Nel progetto del controllore consumatore, fare clic con il pulsante destro del mouse sul controllore produttore e selezionare Module Properties.

6. Fare clic su ... per aprire la finestra di dialogo Safety Network Number.

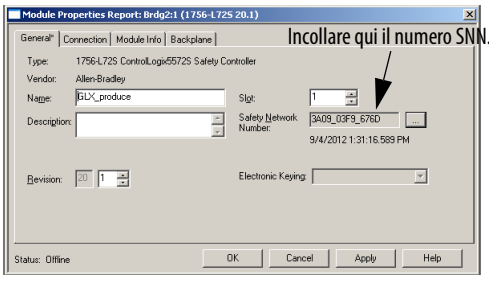
7. Incollare il numero SNN del controllore produttore nel campo SNN e fare clic su OK.

   A questo punto, i numeri di rete di sicurezza corrispondono.

Finestra di dialogo Controller Properties nel progetto del



Finestra di dialogo Module Properties nel progetto del consumatore



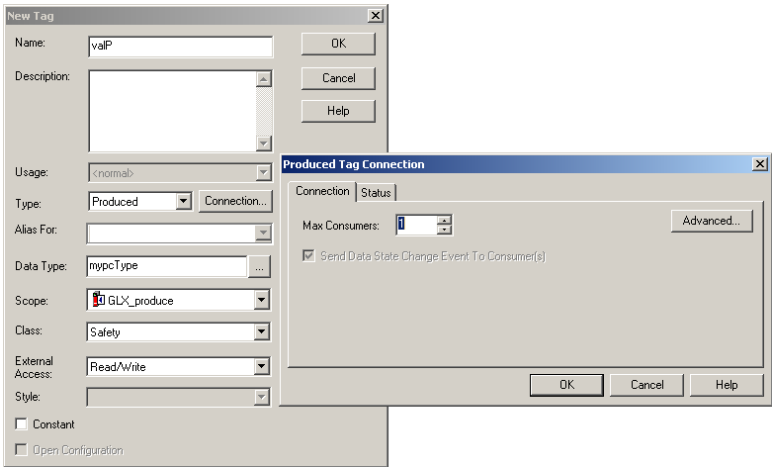
Produzione di un tag di sicurezza

Per produrre un tag di sicurezza, attenersi alla seguente procedura.

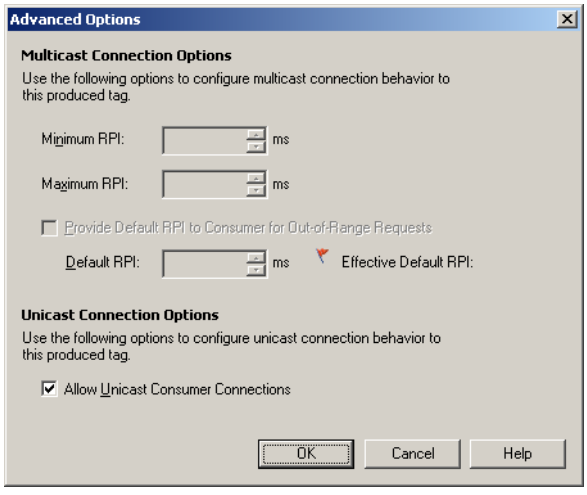
1. Nel progetto del controllore produttore, creare un tipo di dati definito dall'utente per definire la struttura dei dati da produrre.

   Assicurarsi che il primo membro dei dati abbia CONNECTION_STATUS come tipo di dati.

2. Fare clic con il pulsante destro del mouse su Controller Tags e selezionare New Tag.
3. Impostare il tipo su Produced, la classe su Safety e il Data Type sul tipo definito dall'utente e creato al punto 1.
4. Fare clic su Connection e inserire il numero di consumatori.



5. Fare clic su Advanced se si desidera cambiare il tipo di connessione deselezionando "Allow Unicast Consumer Connections".



6. Fare clic su OK.

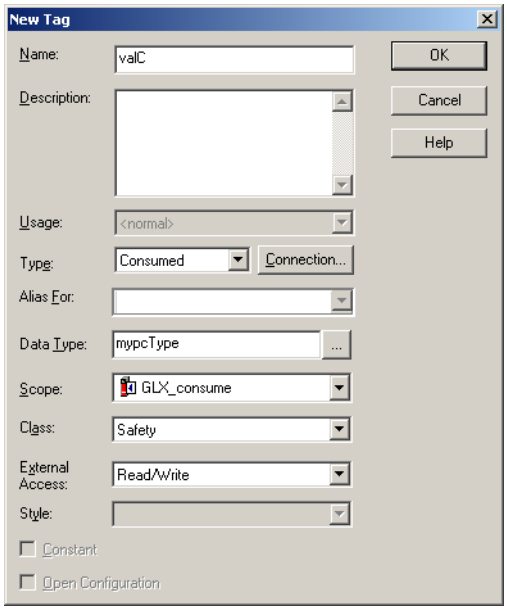
Consumo di dati tag di sicurezza

Per consumare i dati prodotti da un altro controllore, attenersi ai seguenti punti.

1. Nel progetto del controllore consumatore, creare un tipo di dati definito dall'utente identico a quello creato nel progetto del produttore.

   SUGGERIMENTO Il tipo di dati definito dall'utente può essere copiato dal progetto del produttore e incollato nel progetto del consumatore.

2. Fare clic con il pulsante destro del mouse su Controller Tags e selezionare New Tag.
3. Impostare il tipo su Consumed, la classe su Safety e Data Type sul tipo di dati definito dall'utente e creato al punto 1.



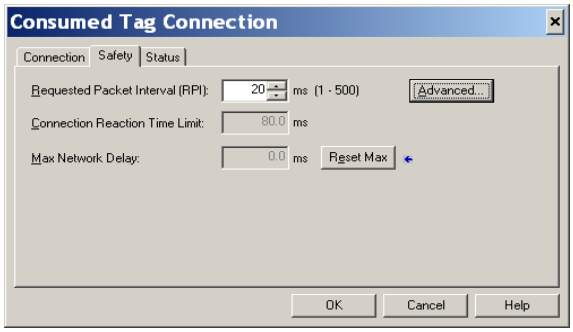
4. Fare clic su Connection per aprire la finestra di dialogo Consumed Tag Connection.

5. Nel menu a discesa Producer, selezionare il controllore che produce i dati.
6. Nel campo Remote Data, immettere il nome del tag prodotto.
7. Fare clic sulla scheda Safety.

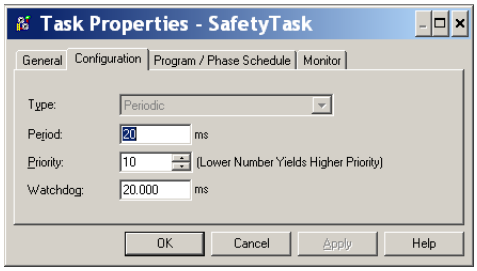
8. Nel campo Requested Packet Interval (RPI), immettere l'intervallo RPI per la connessione, espresso tramite incrementi di 1 ms.

   Il valore predefinito è 20 ms.

Progetto del consumatore



Progetto del produttore

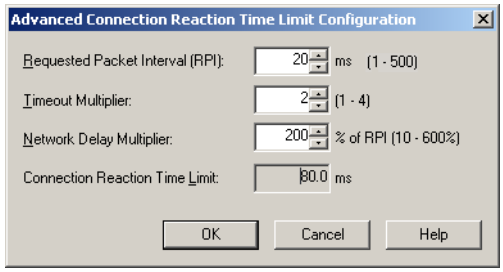


L'intervallo RPI specifica il periodo tra gli aggiornamenti dei dati su una determinata connessione. L'intervallo RPI del tag di sicurezza consumato deve essere identico al periodo del task di sicurezza del progetto di sicurezza produttore.

Il limite del tempo di risposta della connessione è la durata massima dei pacchetti di sicurezza sulla connessione associata. Per semplici requisiti di temporizzazione, è possibile modificare l'intervallo RPI per ottenere un tempo limite di risposta della connessione accettabile.

Il parametro Max Network Delay corrisponde al massimo ritardo di trasferimento osservato dal momento in cui i dati sono stati prodotti fino al momento in cui sono stati ricevuti. Se online, fare clic su Reset Max per ripristinare il ritardo di rete massimo.

9. Se il limite del tempo di risposta della connessione è accettabile, fare clic su OK; per requisiti più complessi, fare clic su Advanced per impostare i parametri di Advanced Connection Reaction Time Limit.



Il parametro Timeout Multiplier determina il numero di RPI di attesa di un pacchetto prima di dichiarare il timeout della connessione.

Il parametro Network Delay Multiplier definisce il tempo di trasferimento del messaggio applicato dal protocollo CIP Safety. Esso specifica il ritardo del percorso produttore-consumatore-produttore. È possibile utilizzare Network Timeout Multiplier per aumentare o ridurre Connection Reaction Time Limit.

Tabella 31 – Altre risorse

Risorsa	Descrizione
Pagine 67…69	Fornisce ulteriori informazioni sull'impostazione dell'RPI e sulla comprensione della modalità con cui i parametri Max. Network Delay, Timeout Multiplier e Network Delay Multipliers influiscono sul tempo di risposta della connessione
Capitolo 9	Contiene ulteriori informazioni sul tipo di dati predefinito CONNECTION_STATUS
Logix5000 Controllers Produced and Consumed Tags Programming Manual, pubblicazione 1756-PM011	Fornisce informazioni dettagliate sull'utilizzo di tag prodotti e consumati

Mappatura dei tag di sicurezza

Non è possibile accedere ai tag standard nell'ambito del controllore con una routine di sicurezza. Per poter utilizzare i dati di tag standard all'interno di routine di task di sicurezza, i controllori GuardLogix dispongono di una funzione di mappatura dei tag di sicurezza che consente di copiare i valori dei tag standard nella memoria dei tag di sicurezza.

Restrizioni

La mappatura dei tag di sicurezza è soggetta alle seguenti restrizioni:

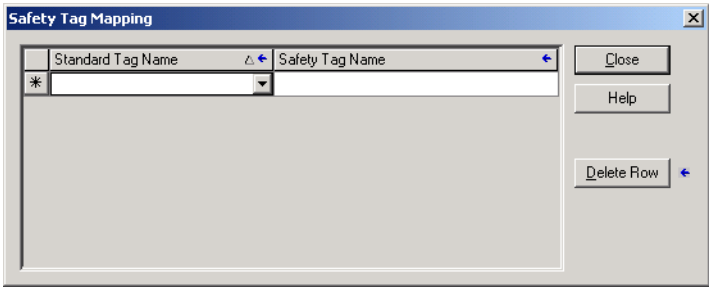
- La coppia tag di sicurezza-tag standard deve essere definita nell'ambito del controllore.
- I tipi di dati della coppia tag di sicurezza-tag standard devono corrispondere.
- Non è consentito l'uso di tag alias.
- La mappatura deve essere definita per l'intero tag. Ad esempio, non è consentito l'uso di myTimer.pre se myTimer è un tag TIMER.
- Una coppia di mappatura è costituita da un tag standard mappato ad un tag di sicurezza.
- Non è possibile mappare un tag standard ad un tag di sicurezza designato come costante.
- La mappatura di tag non può essere modificata in presenza delle seguenti condizioni:
  - se il progetto è in blocco di sicurezza
  - se esiste una firma del task di sicurezza
  - se il selettore a chiave è in posizione RUN
  - se si è verificato un errore di sicurezza irreversibile
  - se la relazione tra il controllore principale e il coprocessore di sicurezza non è valida.

ATTENZIONE: Se si utilizzano i dati standard in una routine di sicurezza, è necessario verificare che i dati vengano utilizzati in modo adeguato. L'utilizzo di dati standard in un tag di sicurezza non li rende dati di sicurezza. Non si può controllare direttamente un'uscita di sicurezza SIL 3/PLe con i dati di tag standard.

Per ulteriori informazioni, consultare Manuale di riferimento per la sicurezza - Sistemi di controllo GuardLogix 5570, pubblicazione 1756-RM099B-IT-P.

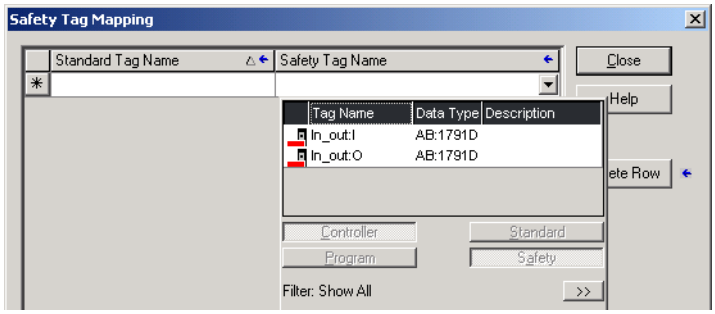
Creazione di coppie di mappatura di tag

1. Per accedere alla finestra di dialogo Safety Tag Mapping, selezionare Map Safety Tags dal menu Logic.



2. Aggiungere un tag esistente nella colonna Standard Tag Name or Safety Tag Name digitando il nome del tag nella cella o selezionando un tag dal menu a tendina.

   Fare clic sulla freccia per visualizzare una finestra di dialogo di esplorazione dei tag filtrati. Nella colonna Standard Tag Name è possibile selezionare solo tag standard definiti nell'ambito del controllore. Nella colonna Safety Tag Name è possibile selezionare solo tag di sicurezza definiti nell'ambito del controllore.



3. Aggiungere un nuovo tag nella colonna Standard Tag Name o Safety Tag Name facendo clic con il pulsante destro del mouse nella cella vuota, selezionando New Tag e digitando il nome del tag nella cella.
4. Fare clic con il pulsante destro del mouse nella cella e selezionare New tagname, dove tagname corrisponde al testo digitato nella cella.

Controllo dello stato della mappatura dei tag

Nell'ultima colonna a sinistra della finestra di dialogo Safety Tag Mapping è indicato lo stato della coppia mappata.

Tabella 32 – Icone dello stato di mappatura dei tag

Contenuto della cella	Descrizione
Vuota	La mappatura dei tag è valida.
	Durante il funzionamento offline, l'icona raffigurante una X indica che la mappatura dei tag non è valida. È possibile spostarsi su una nuova riga o chiudere la finestra di dialogo Safety Tag Mapping.(1) Durante il funzionamento online, una mappa di tag non valida causa un messaggio di errore in cui viene indicato il motivo per il quale la mappatura non è valida. Non è possibile spostarsi su un'altra riga o chiudere la finestra di dialogo Safety Tag Mapping nel caso in cui sia presente un errore di mappatura dei tag.
	Indica la riga attiva.
	Indica la riga Create New Mapped Tag.
	Indica una modifica in sospeso.

(1) La mappatura dei tag viene controllata anche durante la verifica del progetto. La presenza di una mappatura di tag non valida causa un errore di verifica del progetto.

Per ulteriori informazioni, vedere le restrizioni relative alla mappatura dei tag a pagina 98.

Protezione dell'applicazione di sicurezza

Per proteggere il programma applicativo da modifiche non autorizzate è possibile attivare il blocco di sicurezza del controllore e generare e registrare la firma del task di sicurezza.

Blocco di sicurezza del controllore

Il controllore GuardLogix può essere impostato in blocco di sicurezza allo scopo di impedire modifiche ai componenti di controllo correlati alla sicurezza. La funzione di blocco di sicurezza può essere utilizzata solo con i componenti di sicurezza, come il task di sicurezza, i programmi di sicurezza, le routine di sicurezza, le istruzioni Add-On di sicurezza, i tag di sicurezza, l'I/O di sicurezza e la firma del task di sicurezza.

Quando il controllore è in blocco di sicurezza, non è possibile eseguire le operazioni indicate di seguito nella sezione dell'applicazione riservata alla sicurezza:

- Programmazione o modifica online/offline (incluse le istruzioni Add-On di sicurezza)
- Forzatura degli I/O di sicurezza
- Modifica dello stato di inibizione degli I/O di sicurezza o delle connessioni prodotte
- Manipolazione dei dati di sicurezza (ad eccezione della logica delle routine di sicurezza)
- Generazione o eliminazione della firma del task di sicurezza

SUGGERIMENTO Il testo relativo al pulsante dello stato di sicurezza sulla barra di stato indica lo stato del blocco di sicurezza.

Nella barra delle applicazioni vengono inoltre visualizzate le icone riportate di seguito ad indicare lo stato di blocco di sicurezza del controllore di sicurezza.

- = controllore in blocco di sicurezza
- = controllore non in blocco di sicurezza

È possibile impostare il blocco di sicurezza del progetto del controllore indipendentemente dalla modalità di funzionamento (online o offline) e a prescindere dalla disponibilità del sorgente del programma, purché non siano presenti forzature di sicurezza o modifiche di sicurezza online in sospeso.

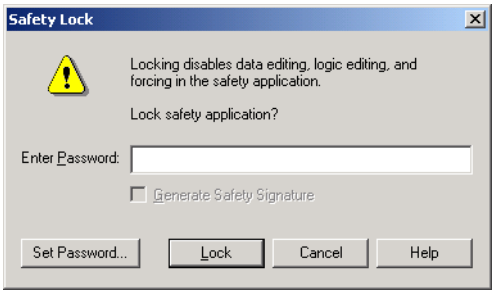
Lo stato in blocco di sicurezza o sblocco di sicurezza non può essere modificato se il selettore a chiave è in posizione RUN.

SUGGERIMENTO Le azioni di attivazione e disattivazione del blocco di sicurezza vengono incluse nel registro del controllore.

Per ulteriori informazioni sull'accesso al registro del controllore, consultare Logix5000 Controllers Controller Information and Status Programming Manual, pubblicazione 1756-PM015.

È possibile attivare e disattivare il blocco di sicurezza del controllore mediante la scheda Safety della finestra di dialogo Controller Properties oppure selezionando Tools>Safety>Safety Lock/Unlock.

Figura 27 – Blocco di sicurezza del controllore



Se la funzione di blocco di sicurezza viene utilizzata tramite l'impostazione di una password, occorre inserirla nel campo Enter Password. In caso contrario, fare clic su Lock.

Nella finestra di dialogo Safety Lock è inoltre possibile impostare o modificare la password. Vedere a pagina 42.

La funzione di blocco di sicurezza descritta in questa sezione e le funzioni di sicurezza standard nell'applicazione Logix Designer sono applicabili ai progetti dei controllori GuardLogix.

Per informazioni sulle funzioni di sicurezza di Logix Designer, consultare il manuale di programmazione Protezione dei controllori Logix5000, pubblicazione 1756-PM016E-IT-P.

Generazione di una firma del task di sicurezza

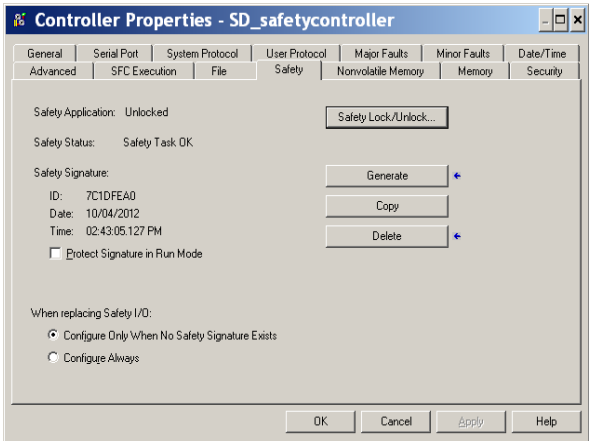
Prima di eseguire il test di verifica, è necessario generare la firma del task di sicurezza. La firma del task di sicurezza può essere generata solo se si è online, con il controllore GuardLogix non in blocco di sicurezza in modalità di programmazione e se non sono presenti forzature di sicurezza, modifiche online di sicurezza in sospeso o errori di sicurezza. Lo stato di sicurezza deve essere Safety Task OK.

Inoltre, è impossibile generare una firma del task di sicurezza se il controllore è in modalità Esecuzione con la protezione della modalità Esecuzione abilitata.

SUGGERIMENTO Per visualizzare lo stato di sicurezza, utilizzare il pulsante di stato di sicurezza sulla barra online (vedere a pagina 120) oppure accedere alla scheda Safety nella finestra di dialogo Controller Properties, come mostrato a pagina 102.

Per generare la firma del task di sicurezza, fare clic su Generate nella scheda Safety della finestra di dialogo Controller Properties. È possibile selezionare anche Tools>Safety>Generate Signature.

Figura 28 – Scheda Safety



Se esiste una firma precedente, viene richiesto di sovrascriverla.

SUGGERIMENTO La creazione e l'eliminazione di una firma del task di sicurezza vengono registrate nel registro del controllore.

Per ulteriori informazioni sulla consultazione del registro del controllore, consultare Logix5000 Controllers Controller Information and Status Programming Manual, pubblicazione 1756-PM015.

Se è presente una firma del task di sicurezza, non è possibile eseguire le seguenti azioni nella sezione relativa alla sicurezza dell'applicazione:

- Programmazione o modifica online/offline (incluse le istruzioni Add-On di sicurezza)
- Forzatura degli I/O di sicurezza
- Modifica dello stato di inibizione degli I/O di sicurezza o dei controllori produttori
- Manipolazione dei dati di sicurezza (ad eccezione della logica delle routine di sicurezza)

Copia della firma del task di sicurezza

È possibile utilizzare il pulsante Copy per creare un record della firma del task di sicurezza da utilizzare per la documentazione, il confronto e la convalida di un progetto di sicurezza. Fare clic su Copy per copiare i componenti ID, Date e Time negli Appunti di Windows.

Eliminazione della firma del task di sicurezza

Fare clic su Delete per eliminare la firma del task di sicurezza. La firma del task di sicurezza non può essere eliminata nei seguenti casi:

- Il controllore è in blocco di sicurezza.
- Il controllore è in modalità Esecuzione con il selettore a chiave su RUN.
- Il controllore è in modalità Esecuzione o Esecuzione remota con la protezione della modalità di esecuzione abilitata.

ATTENZIONE: Se si elimina la firma del task di sicurezza, occorre testare e convalidare nuovamente il sistema per verificarne la conformità al livello SIL 3/PLe.

Per ulteriori informazioni sui requisiti SIL 3/PLe, consultare Manuale di riferimento per la sicurezza - Sistemi di controllo GuardLogix 5570, pubblicazione 1756-RM099B-IT-P.

Programmazione delle restrizioni

Le restrizioni che limitano la disponibilità di alcune voci di menu e funzioni (ossia le funzioni Taglia, Incolla, Elimina, Trova e sostituisci) vengono imposte dall'applicazione Logix Designer allo scopo di proteggere da modifiche i componenti di sicurezza nei seguenti casi:

- Il controllore è in blocco di sicurezza.
- Esiste una firma del task di sicurezza.
- Sono presenti errori di sicurezza.
- Lo stato di sicurezza è uno dei seguenti:
  - Coprocessore mancante
  - Coprocessore non disponibile
  - Hardware incompatibile
  - Firmware incompatibile

Se si verifica anche solo una di queste condizioni, non è possibile:

- Creare o modificare gli oggetti di sicurezza, ivi compresi programmi di sicurezza, routine di sicurezza, tag di sicurezza, istruzioni Add-On di sicurezza e dispositivi I/O di sicurezza.

  IMPORTANTE I tempi di scansione del task e dei programmi di sicurezza possono essere reimpostati in modalità online.

- Applicare forzature ai tag di sicurezza.
- Creare nuove mappature dei tag di sicurezza.
- Modificare o eliminare mappature di tag.
- Modificare o eliminare tipi di dati definiti dall'utente utilizzati dai tag di sicurezza.

- Modificare il nome, la descrizione, il tipo di chassis, lo slot e il Numero Rete di Sicurezza (SNN) del controllore.
- Modificare o eliminare la firma del task di sicurezza mentre è attivo il blocco di sicurezza.

Collegamento online con il controllore

Argomento	Pagina
Connessione del controllore alla rete	105
Analisi dei fattori che influiscono sul collegamento online	106
Download	108
Upload	110
Collegamento online	111

Connessione del controllore alla rete

Connettere il controllore alla rete, se non è stato collegato.

Tabella 33 - Connessioni di comunicazione

Per questo tipo di connessione	Usare	Vedere
USB	Cavo USB 2.0	Collegamenti di comunicazione a pagina 29
EtherNet/IP	Dispositivo EtherNet/IP in uno slot libero nello stesso chassis del controllore	Connessione del dispositivo EtherNet/IP e del computer a pagina 105
DeviceNet	Modulo 1756-DNB in uno slot libero nello stesso chassis del controllore	Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer a pagina 106
ControlNet	Modulo 1756-CN2 in uno slot libero nello stesso chassis del controllore	

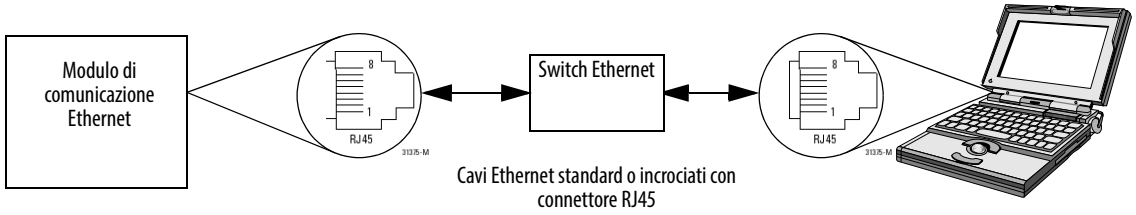
Connessione del dispositivo EtherNet/IP e del computer

AVVERTENZA: Se si connette o si disconnette il cavo di comunicazione con il modulo o qualsiasi dispositivo sulla rete alimentato, può verificarsi un arco elettrico, Ciò può provocare un'esplosione in caso di installazioni in aree pericolose.

Prima di procedere, assicurarsi di aver tolto l'alimentazione o che l'area non sia pericolosa.

Connettere il dispositivo EtherNet/IP e il computer utilizzando un cavo Ethernet.

Figura 29 – Connessioni Ethernet



Connessione del modulo di comunicazione ControlNet o dello scanner DeviceNet e del computer

Per accedere alla rete ControlNet o DeviceNet, è possibile:

- Eseguire la connessione direttamente alla rete.
- Eseguire la connessione a una rete seriale o EtherNet/IP e passare (ponte) alla rete richiesta. Per eseguire questa operazione, non è necessaria programmazione aggiuntiva.

Configurazione di un driver EtherNet/IP, ControlNet o DeviceNet

Per informazioni sulla configurazione di un driver, consultare la pubblicazione appropriata:

- Moduli EtherNet/IP in sistemi di controllo Logix5000 Manuale dell'utente, pubblicazione ENET-UM001L-IT-P
- ControlNet Modules in Logix5000 Control Systems User Manual, pubblicazione CNET-UM001
- DeviceNet Modules in Logix5000 Control Systems, pubblicazione DNET-UM004

Analisi dei fattori che influiscono sul collegamento online

L'applicazione Logix Designer determina se è possibile collegarsi in linea con un controllore di destinazione a seconda che il progetto offline sia nuovo o siano state apportate modifiche. Se il progetto è nuovo, è necessario prima scaricarlo nel controllore. Se sono state apportate modifiche al progetto, verrà richiesto di effettuare l'upload o il download. Se non sono state apportate modifiche, è possibile collegarsi online per controllare l'esecuzione del progetto.

Diversi fattori influiscono su questi processi, compresa la funzione di corrispondenza tra progetto e controllore, lo stato di sicurezza e gli errori, l'esistenza di una firma del task di sicurezza e lo stato di blocco/sblocco di sicurezza del progetto e del controllore.

Corrispondenza tra progetto e controllore

La funzione di corrispondenza tra progetto e controllore influisce sui processi di download, upload e collegamento online di progetti standard e di sicurezza.

Se la funzione di corrispondenza tra progetto e controllore è abilitata nel progetto offline, l'applicazione Logix Designer confronta il numero seriale del controllore nel progetto offline con quello del controllore connesso. Se non corrispondono, è necessario annullare il download/l'upload, eseguire la connessione al controllore corretto, oppure confermare di essere collegati al controllore corretto per aggiornare il numero seriale nel progetto, in modo che corrisponda al controllore di destinazione.

Corrispondenza della versione del firmware

La corrispondenza della versione del firmware influisce sul processo di download. Se la versione del controllore non corrisponde a quella del progetto, verrà richiesto di aggiornare il firmware del controllore. L'applicazione Logix Designer consente di aggiornare il firmware nell'ambito della sequenza di download.

IMPORTANTE	Per aggiornare il firmware del controllore, è necessario prima installare un kit di aggiornamento del firmware. Un kit di aggiornamento viene spedito in un DVD supplementare insieme a Studio 5000.

SUGGERIMENTO	Per aggiornare il firmware è anche possibile selezionare ControlFlash dal menu Tools dell'applicazione Logix Designer.

Stato di sicurezza/errori

L'upload della logica di programma e il collegamento online sono consentiti indipendentemente dallo stato di sicurezza. Lo stato di sicurezza e gli errori influiscono solo sul processo di download.

È possibile visualizzare lo stato di sicurezza dalla scheda Safety nella finestra di dialogo Controller Properties.

Firma del task di sicurezza e stato di blocco/sblocco di sicurezza

L'esistenza di una firma del task di sicurezza e lo stato di blocco/sblocco di sicurezza del controllore influiscono sia sui processi di upload sia su quelli di download.

Durante l'upload

Se il controllore ha una firma del task di sicurezza, quest'ultima e lo stato di blocco del task di sicurezza vengono caricati con il progetto. Ad esempio, se il progetto nel controllore non era in blocco di sicurezza, il progetto offline rimane tale dopo l'upload, anche se era bloccato prima dell'upload.

In seguito ad un upload, la firma del task di sicurezza nel progetto offline corrisponde alla firma del task di sicurezza nel controllore.

Durante il download

L'esistenza di una firma del task di sicurezza e lo stato di blocco di sicurezza del controllore determinano la possibilità di eseguire o meno un download.

Tabella 34 - Effetto del blocco di sicurezza e della firma del task di sicurezza sull'operazione di download

Stato del blocco di sicurezza	Stato della firma del task di sicurezza	Funzionalità di download
Controllore non in blocco di sicurezza	La firma del task di sicurezza nel progetto offline corrisponde alla firma del task di sicurezza nel controllore.	Vengono scaricati tutti i componenti standard del progetto. I tag di sicurezza vengono reinizializzati ai valori presenti al momento della creazione della firma del task di sicurezza. Il task di sicurezza non viene scaricato. Lo stato del blocco di sicurezza corrisponde allo stato nel progetto offline.
	Le firme del task di sicurezza non corrispondono.	Se il controllore aveva una firma del task di sicurezza, quest'ultima viene cancellata automaticamente e viene scaricato l'intero progetto. Lo stato del blocco di sicurezza corrisponde allo stato nel progetto offline.
Controllore in blocco di sicurezza	Le firme del task di sicurezza corrispondono.	Se il progetto offline e il controllore sono in blocco di sicurezza, vengono scaricati tutti i componenti standard del progetto e il task di sicurezza viene reinizializzato con i valori presenti al momento della creazione della firma del task di sicurezza. Se il progetto offline non è in blocco di sicurezza, ma il controllore lo è, il download viene bloccato e per proseguire occorre prima sbloccare il controllore.
	Le firme del task di sicurezza non corrispondono.	È necessario innanzitutto lo sblocco di sicurezza del controllore per consentire il download. Se il controllore aveva una firma del task di sicurezza, quest'ultima viene cancellata automaticamente e viene scaricato l'intero progetto. Lo stato del blocco di sicurezza corrisponde allo stato nel progetto offline.

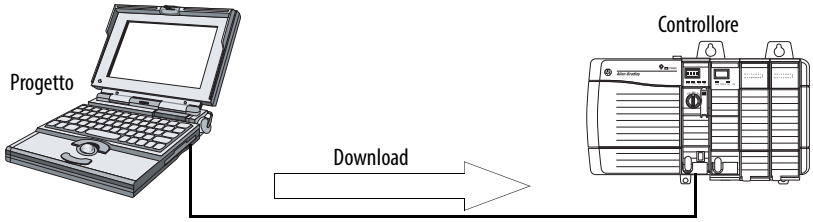
IMPORTANTE Durante il download su un controllore non in blocco di sicurezza, se il firmware del controllore differisce da quello del progetto offline, adottare una delle seguenti soluzioni:

- Aggiornare il controllore in modo che corrisponda al progetto offline. Una volta completato l'aggiornamento, l'intero progetto viene scaricato.
- Aggiornare il progetto alla versione del controllore.

Se si aggiorna il progetto, la firma del task di sicurezza viene cancellata ed è necessario ripetere la convalida del sistema.

Download

Per trasferire il progetto dal computer al controllore, attenersi alla seguente procedura.



1. Portare il selettore a chiave del controllore su REM.
2. Aprire il progetto del controllore da scaricare.
3. Definire il percorso al controllore.
   a. Fare clic su Who Active .
   b. Selezionare il controllore.
   Per aprire un livello, fare clic sul segno +. Se è già stato selezionato un controllore, assicurarsi che si tratti del controllore corretto.

4. Fare clic su Download.

   L'applicazione Logix Designer confronta le seguenti informazioni nel progetto offline e nel controllore:
   - Numero seriale del controllore (se è selezionata la corrispondenza tra progetto e controllore)
   - Versioni principale e secondaria del firmware
   - Stato di sicurezza
   - Firma del task di sicurezza (se presente)
   - Stato del blocco di sicurezza

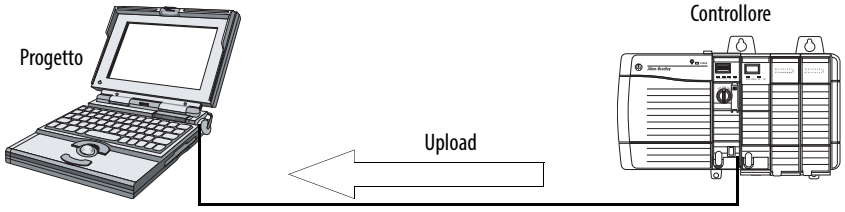
5. Per completare il download in base alle risposte dell'applicazione Logix Designer, attenersi alle istruzioni riportate nella seguente tabella.

Se nel software è presente la seguente indicazione	Procedere come segue
Download nel controllore.	Scegliere Download. Il progetto viene scaricato nel controllore e si collega online.
Impossibile eseguire il download nel controllore. Mancata corrispondenza tra il numero seriale del progetto offline e il numero seriale del controllore. Il controllore selezionato può non essere corretto.	Eseguire la connessione al controllore corretto oppure verificare che il controllore utilizzato sia quello corretto. Se si tratta del controllore corretto, contrassegnare la casella di controllo "Update project serial number" per consentire l'esecuzione del download. Il numero seriale del progetto viene modificato in modo da corrispondere al numero seriale del controllore.
Impossibile eseguire il download nel controllore. La versione principale del progetto offline e il firmware del controllore non sono compatibili.	Selezionare Update Firmware. Selezionare la versione richiesta e fare clic su Update. Per confermare la selezione, fare clic su Yes.
Impossibile eseguire il download nel controllore. Coprocessore di sicurezza mancante o non disponibile.	Annullare il processo di download. Installare un coprocessore di sicurezza compatibile prima di eseguire il download.
Impossibile eseguire il download nel controllore. La versione del firmware del coprocessore di sicurezza non è compatibile con il controllore primario.	Aggiornare la versione del firmware del coprocessore di sicurezza. Selezionare Update Firmware. Selezionare la versione richiesta e fare clic su Update. Per confermare la selezione, fare clic su Yes.
Impossibile eseguire il download nel controllore. La connessione di sicurezza non è stata stabilita.	Annullare il processo di download e provare ad eseguire un nuovo download.
Impossibile eseguire il download nel controllore. La firma del task di sicurezza non compatibile non può essere eliminata quando il progetto è in blocco di sicurezza.	Annullare il processo di download. Per eseguire il download del progetto, è necessario disattivare il blocco di sicurezza del progetto offline, eliminare la firma del task di sicurezza e quindi scaricare il progetto. **IMPORTANTE:** il sistema di sicurezza richiede una nuova convalida.
Impossibile eseguire il download mantenendo la firma del task di sicurezza. La versione secondaria del firmware del controllore non è compatibile con la firma del task di sicurezza del progetto offline.	• Se la versione secondaria del firmware non è compatibile, per mantenere la firma del task di sicurezza, aggiornare la versione del firmware nel controllore in modo che corrisponda esattamente al progetto offline. Scaricare quindi il progetto offline. • Per procedere con il download indipendentemente dall'incompatibilità della firma del task di sicurezza, fare clic su Download. La firma del task di sicurezza viene cancellata. **IMPORTANTE:** il sistema di sicurezza richiede una nuova convalida.
Impossibile eseguire il download nel controllore. Il controllore è bloccato. Le firme del task di sicurezza del controllore e del progetto offline non corrispondono.	Selezionare Unlock. Viene visualizzata la finestra di dialogo Safety Unlock for Download. Se la casella di controllo Delete Signature è contrassegnata e si seleziona Unlock, per confermare l'eliminazione, fare clic su Yes.
Si verificherà un errore di sicurezza irreversibile sul controllore di sicurezza. Non è stato designato un master CST (tempo di sistema coordinato).	Selezionare Enable Time Synchronization e fare clic su Download per procedere.

Se il download viene eseguito correttamente, lo stato di blocco di sicurezza e la firma del task di sicurezza del controllore corrispondono al progetto scaricato. I dati di sicurezza vengono inizializzati ai valori esistenti al momento della creazione della firma del task di sicurezza.

Upload

Per trasferire un progetto dal controllore al computer, attenersi alla seguente procedura.



1. Definire il percorso al controllore.
   a. Fare clic su Who Active .
   b. Selezionare il controllore.
   Per espandere un livello, fare clic sul segno +. Se è già stato selezionato un controllore, assicurarsi che si tratti del controllore corretto.
2. Fare clic su Upload.
3. Se il file di progetto non esiste, selezionare File>Select>Yes.
4. Se il file di progetto è già stato creato, selezionarlo.

   Se è attivata la corrispondenza tra il progetto e il controllore, l'applicazione Logix Designer controlla se il numero seriale del progetto aperto e il numero seriale del controllore corrispondono.

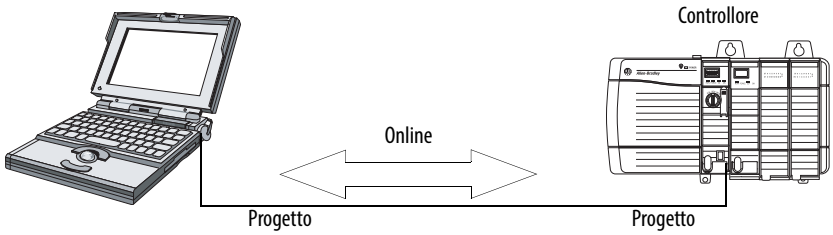
   Se i numeri seriali del controllore non corrispondono, è possibile procedere in uno dei seguenti modi:
   - Annullare l'upload ed eseguire la connessione a un controllore corrispondente. Dopodiché, avviare nuovamente la procedura di upload.
   - Selezionare un nuovo progetto da caricare oppure selezionare un altro progetto scegliendo Select File.
   - Aggiornare il numero seriale del progetto in modo che corrisponda al controllore selezionando la casella di controllo Update Project Serial Number, quindi l'opzione Upload.
5. L'applicazione Logix Designer controlla se il progetto aperto corrisponde al progetto del controllore.
   a. Se i progetti non corrispondono, è necessario selezionare un file corrispondente oppure annullare il processo di upload.
   b. Se i progetti corrispondono, il software controlla se sono state apportate modifiche al progetto offline (aperto).
6. L'applicazione Logix Designer verifica la presenza di modifiche nel progetto offline.
   a. Se non sono state apportate modifiche al progetto offline, è possibile collegarsi online senza eseguire l'upload. Fare clic su Go Online.
   b. Se sono state apportate modifiche al progetto aperto non presenti nel controllore, è possibile scegliere di caricare il progetto, annullare l'upload oppure selezionare un altro file.

Se si seleziona Upload, vengono caricate le applicazioni standard e di sicurezza. Se è stata configurata una firma del task di sicurezza, anch'essa viene caricata. Lo stato del blocco di sicurezza del progetto riflette lo stato originale del progetto in linea (controllore).

SUGGERIMENTO Prima di eseguire l'upload, se è presente una firma del task di sicurezza offline oppure il progetto offline è in blocco di sicurezza, ma il controllore non lo è o non dispone di una firma del task di sicurezza, la firma del task di sicurezza offline e lo stato di blocco di sicurezza saranno sostituiti dai valori in linea (sblocco di sicurezza senza firma del task di sicurezza). Se non si desidera apportare tali modifiche in modo permanente, non salvare il progetto offline al termine dell'upload.

Collegamento online

Per passare online e monitorare un progetto in esecuzione sul controllore, attenersi alla seguente procedura.



1. Definire il percorso al controllore.
   a. Fare clic su Who Active .
   b. Selezionare il controllore.
   Per espandere un livello, fare clic sul segno +. Se è già stato selezionato un controllore, assicurarsi che si tratti del controllore corretto.
2. Fare clic su Go Online.

   L'applicazione Logix Designer controlla quanto segue:
   - I numeri seriali del progetto offline e del controllore corrispondono (se è selezionata la funzione di corrispondenza tra il progetto ed il controllore)?
   - Il progetto offline contiene modifiche non presenti nel progetto del controllore?
   - Le versioni del progetto offline e del firmware del controllore corrispondono?
   - Il progetto offline o il controllore sono in blocco di sicurezza?
   - Il progetto offline e il controllore hanno firme del task di sicurezza compatibili?

3. Per connettersi al controllore, seguire le indicazioni riportate nella tabella seguente.

Tabella 35 - Connessione al controllore

Se nel software è presente la seguente indicazione	Procedere come segue
Impossibile eseguire la connessione al controllore. Mancata corrispondenza tra il numero seriale del progetto offline e quello del controllore. Il controllore selezionato può non essere quello corretto.	Eseguire la connessione al controllore corretto, selezionare un altro file di progetto oppure selezionare la casella di controllo "Update project serial number" e scegliere Go Online… per eseguire la connessione al controllore e aggiornare il numero seriale del progetto offline in modo che corrisponda al controllore.
Impossibile eseguire la connessione al controllore. La versione del progetto offline e il firmware del controllore non sono compatibili.	Scegliere una delle seguenti opzioni: • Selezionare Update Firmware. Selezionare la versione richiesta e fare clic su Update. Per confermare la selezione, fare clic su Yes. **IMPORTANTE:** il progetto online viene eliminato. • Per mantenere il progetto online, annullare il processo online e installare una versione di Studio 5000 compatibile con la versione del firmware del controllore.
È necessario eseguire l'upload o il download per collegarsi online utilizzando il progetto aperto.	Scegliere una delle seguenti opzioni: • Upload per aggiornare il progetto offline. • Download per aggiornare il progetto del controllore. • Selezionare File per selezionare un altro progetto offline.
Impossibile eseguire la connessione mantenendo la firma del task di sicurezza. La versione secondaria del firmware del controllore non è compatibile con la firma del task di sicurezza del progetto offline.	• Per mantenere la firma del task di sicurezza quando la versione secondaria del firmware non è compatibile, aggiornare la versione del firmware nel controllore in modo che corrisponda esattamente al progetto offline. Collegarsi quindi online al controllore. • Per procedere con il download indipendentemente dall'incompatibilità della firma del task di sicurezza, fare clic su Download. La firma del task di sicurezza viene cancellata. **IMPORTANTE:** il sistema di sicurezza richiede una nuova convalida.
Impossibile eseguire la connessione al controllore. La firma del task di sicurezza non compatibile non può essere eliminata mentre il progetto è in blocco di sicurezza.	Annullare il processo online. È necessario disattivare il blocco di sicurezza del progetto offline prima del collegamento online.

Quando il controllore e l'applicazione Logix Designer sono online, lo stato di blocco di sicurezza e la firma del task di sicurezza del controllore corrispondono al progetto del controllore. Lo stato del blocco di sicurezza e la firma del task di sicurezza del progetto non online vengono sovrascritti dal controllore. Se non si desidera apportare tali modifiche al progetto offline in modo permanente, non salvare il file di progetto al termine del collegamento online.

Memorizzazione e caricamento di progetti con la memoria non volatile

Argomento	Pagina
Utilizzo delle schede di memoria per la memoria non volatile	113
Memorizzazione di un progetto di sicurezza	114
Caricamento di un progetto di sicurezza	115
Utilizzo dei moduli di alimentazione	116
Valutazione dell'alimentazione dell'orologio interno (WallClockTime) da parte del modulo ESM	118
Gestione del firmware con Firmware Supervisor	118

Utilizzo delle schede di memoria per la memoria non volatile

I controllori GuardLogix 5570 supportano una scheda di memoria per la memoria non volatile. La memoria non volatile consente di mantenere una copia del progetto sul controllore. Il controllore non richiede alimentazione o una batteria per il mantenimento di questa copia.

Il progetto memorizzato può essere caricato dalla memoria non volatile alla memoria utente del controllore:

- Ad ogni accensione
- Quando non è presente alcun progetto nel controllore e quest'ultimo viene acceso
- In qualunque momento attraverso l'applicazione Logix Designer.

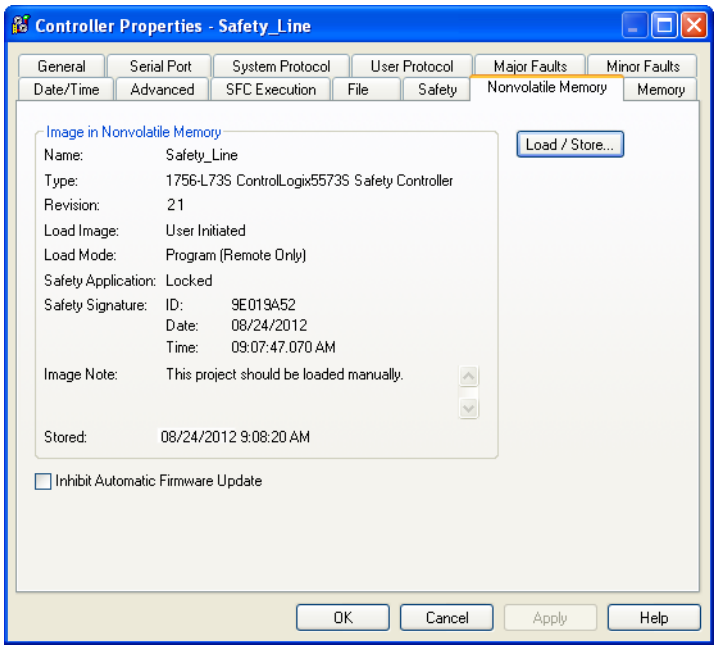
IMPORTANTE Nella memoria non volatile vengono memorizzati i contenuti della memoria utente quando si salva il progetto:

- Le modifiche apportate in seguito alla memorizzazione del progetto non vengono salvate nella memoria non volatile.
- Se si apportano delle modifiche al progetto ma non vengono memorizzate, queste ultime vengono sovrascritte quando si carica il progetto dalla memoria non volatile. In tal caso, è necessario eseguire l'upload o il download del progetto per collegarsi online.
- Per salvare modifiche quali modifiche online, valori dei tag, o una schedulazione della rete ControlNet, è necessario memorizzare nuovamente il progetto in seguito all'esecuzione delle modifiche.

ATTENZIONE: Non rimuovere la scheda di memoria mentre il controllore sta leggendo o scrivendo su di essa, processo indicato dall'indicatore di stato OK che lampeggia in verde. Questa operazione potrebbe provocare il danneggiamento dei dati presenti sulla scheda o nel controllore, o la corruzione dell'ultimo firmware caricato nel controllore. Lasciare la scheda nel controllore finché la luce dell'indicatore di stato OK non diventa verde fissa.

Se è installata una scheda di memoria, è possibile visualizzarne i contenuti tramite la scheda Nonvolatile Memory della finestra di dialogo Controller Properties. Se sulla scheda è memorizzata un'applicazione di sicurezza, vengono visualizzati lo stato del blocco di sicurezza e la firma del task di sicurezza.

Figura 30 – Scheda Nonvolatile Memory



Per informazioni dettagliate sull'utilizzo della memoria non volatile, consultare il manuale di programmazione Logix5000 Controllers Nonvolatile Memory, pubblicazione 1756-PM017.

Memorizzazione di un progetto di sicurezza

Non è possibile memorizzare un progetto di sicurezza se lo stato del task di sicurezza è Safety Task Inoperable. Quando si memorizza un progetto di sicurezza, i firmware del controllore primario e del coprocessore di sicurezza vengono salvati sulla scheda di memoria.

Se nel controllore non è presente alcun progetto applicativo, è possibile salvare il firmware del controllore di sicurezza solo se è stata stabilita un'associazione valida. Il caricamento del solo firmware non determina l'annullamento della condizione Safety Task Inoperable.

Se è presente una firma del task di sicurezza quando si memorizza un progetto, avviene quanto segue:

- I tag di sicurezza vengono memorizzati insieme ai valori presenti al momento della creazione della firma.
- I tag standard vengono aggiornati.
- La firma del task di sicurezza corrente viene salvata.

Quando si memorizza un progetto applicativo di sicurezza su una scheda di memoria, si consiglia di selezionare Program (Remote Only) come modalità di caricamento, ossia la modalità a cui deve passare il controllore in seguito al caricamento.

Caricamento di un progetto di sicurezza

Il caricamento può essere avviato dalla memoria non volatile in presenza delle seguenti condizioni:

- Il tipo di controllore specificato dal progetto memorizzato nella memoria non volatile corrisponde al tipo di controllore.
- Le versioni principale e secondaria del progetto nella memoria non volatile corrispondono alle versioni principali e secondarie del controllore.
- Il controllore non è in modalità Esecuzione.

Esistono varie opzioni relative alle condizioni in cui è possibile caricare il progetto nella memoria utente del controllore.

Tabella 36 – Opzioni di caricamento di un progetto

Se si desidera caricare il progetto	Selezionare questa opzione di Load Image	Note
Ad ogni accensione o in caso di spegnimento e riaccensione	All'accensione	• Durante un ciclo di spegnimento e riaccensione si perdono le eventuali modifiche online, i valori dei tag e la schedulazione della rete non memorizzati nella memoria non volatile. • Il controllore carica il progetto memorizzato e il firmware ad ogni accensione, indipendentemente dal firmware o dal progetto applicativo presenti sul controllore. Il caricamento si verifica indipendentemente dal fatto che il controllore sia in blocco di sicurezza o disponga di una firma del task di sicurezza. • Per caricare il progetto, è sempre possibile utilizzare l'applicazione Logix Designer.
Se non è presente alcun progetto nel controllore e si esegue l'accensione o si disattiva e riattiva l'alimentazione dello chassis	Se la memoria è danneggiata	• Ad esempio, se la batteria si scarica e il controllore non viene alimentato, il progetto viene cancellato dalla memoria. Quando viene ripristinata l'alimentazione, questa opzione di caricamento fa sì che il progetto venga ricaricato nel controllore. • Se è necessario, il controllore aggiorna il firmware sul controllore primario o il coprocessore di sicurezza. Viene anche caricato il progetto applicativo memorizzato nella memoria non volatile e il controllore passa alla modalità selezionata, Programmazione o Esecuzione. • Per caricare il progetto, è sempre possibile utilizzare l'applicazione Logix Designer.
Solo attraverso l'applicazione Logix Designer	Avviato dall'utente	• Se il tipo di controllore e le versioni principali e secondarie del progetto nella memoria non volatile corrispondono al tipo di controllore e alle versioni principali e secondarie del controllore, è possibile avviare un caricamento, indipendentemente dallo stato del task di sicurezza. • È possibile caricare un progetto in un controllore in blocco di sicurezza solo se la firma del task di sicurezza del progetto memorizzato nella memoria non volatile corrisponde al progetto presente nel controllore. • Se le firme non corrispondono o se il controllore è in blocco di sicurezza senza una firma del task di sicurezza, viene richiesto di sbloccare preventivamente il controllore. **IMPORTANTE:** quando si sblocca il controllore e si avvia un caricamento dalla memoria non volatile, lo stato del blocco di sicurezza, le password e la firma del task di sicurezza vengono impostati sui valori contenuti nella memoria non volatile al termine del caricamento. • Se il firmware presente sul controllore primario corrisponde alla versione di quello presente nella memoria non volatile, se necessario, il firmware del coprocessore di sicurezza viene aggiornato, l'applicazione memorizzata nella memoria non volatile viene caricata, così il task di sicurezza assume lo stato Safety Task Operable e il controllore passa alla modalità selezionata, Programmazione o Esecuzione.

IMPORTANTE Prima di usare il software ControlFLASH, verificare che la scheda SD sia sbloccata, se è impostato il caricamento all'accensione. In caso contrario, i dati aggiornati rischiano di essere sovrascritti dal firmware sulla scheda di memoria.

Utilizzo dei moduli di alimentazione

I moduli ESM GuardLogix possono essere utilizzati per quanto segue:

- Alimentare il controllore per salvare il programma nella memoria non volatile (NVS) integrata nel controllore dopo l'interruzione dell'alimentazione allo chassis o la rimozione del controllore da uno chassis alimentato.

  IMPORTANTE Quando si usa un modulo ESM per salvare il programma sulla memoria NVS integrata, il programma **non** viene salvato sulla scheda SD installata nel controllore.

- Cancellare il programma dalla memoria NVS integrata nel controllore. Per ulteriori informazioni, consultare Cancellazione del programma dalla memoria NVS integrata

La tabella che segue descrive i moduli ESM.

Tabella 37 – Moduli di alimentazione

N. catalogo	Descrizione
1756-ESMCAP(XT)	ESM con condensatore I controllori vengono forniti con questo modulo ESM installato.
1756-ESMNSE(XT)	ESM con condensatore senza alimentazione di backup dell'orologio interno (WallClockTime) Utilizzare questo ESM se l'applicazione richiede che il modulo ESM installato riduca l'energia residua a 40 µJ o meno prima di installarlo o rimuoverlo dall'applicazione. Questo modulo ESM, inoltre, può essere utilizzato soltanto con un controllore 1756-L73S (8 MB) o con un controllore di memoria inferiore.
1756-ESMNRM(XT)	ESM di protezione con condensatore (non rimovibile) Questo modulo aumenta il grado di sicurezza dell'applicazione prevenendo l'accesso fisico al connettore USB e alla scheda SD.
1756-SPESMNSE(XT)	ESM con condensatore e senza alimentazione di backup WallClockTime per il coprocessore di sicurezza Utilizzare questo modulo ESM se l'applicazione richiede che il modulo ESM installato riduca l'energia residua a 40 µJ o meno prima di installarlo o rimuoverlo dall'applicazione. Il coprocessore di sicurezza 1756-L7SPXT per temperature estreme viene fornito con il modulo 1756-SPESMNSEXT installato.
1756-SPESMNRM(XT)	ESM di protezione con condensatore (non rimovibile) per il coprocessore di sicurezza

Salvataggio del programma sulla memoria NVS integrata

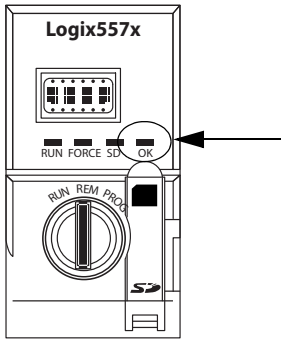
Per salvare il programma sulla memoria NVS quando si interrompe l'alimentazione del controllore, procedere come segue.

1. Interrompere l'alimentazione del controllore.

   L'alimentazione può essere interrotta in due modi:
   - Interrompendo l'alimentazione allo chassis con il controllore installato nello chassis.
   - Rimuovendo il controllore dallo chassis alimentato.

Subito dopo l'interruzione dell'alimentazione del controllore, l'indicatore di stato OK diventa rosso fisso e rimane così per tutto il tempo di salvataggio del programma.

Figura 31 – Indicatore di stato OK.



2. Non rimuovere il modulo ESM dal controllore fino allo spegnimento dell'indicatore di stato OK.

3. Se necessario, rimuovere il modulo ESM dal controllore solo quando l'indicatore di stato OK passa da rosso fisso a spento.

Cancellazione del programma dalla memoria NVS integrata

Se l'applicazione lo consente, cancellare il programma dalla memoria NVS integrata nel controllore effettuando le seguenti operazioni.

1. Rimuovere il modulo ESM dal controllore.

2. Interrompere l'alimentazione del controllore scollegando quella dello chassis in cui il controllore è installato o rimuovendo il controllore da uno chassis alimentato.

3. Reinstallare il modulo ESM nel controllore.

4. Ripristinare l'alimentazione del controllore.
   a. Se il controllore è già installato nello chassis, rialimentare lo chassis.
   b. Se il controllore non è installato nello chassis, reinstallare il controllore nello chassis e rialimentare lo chassis.

Valutazione dell'alimentazione dell'orologio interno (WallClockTime) da parte del modulo ESM

Il modulo ESM supporta il mantenimento dell'attributo WallClockTime del controllore in mancanza di alimentazione. Fare riferimento alla tabella che segue per stimare l'autonomia del modulo ESM in base alla temperatura del controllore e al modulo ESM installato.

Tabella 38 – Temperatura e autonomia

Temperatura	Autonomia (in giorni)		
	1756-ESMCAP(XT)	1756-ESMNRM(XT) 1756-SPESMNRM(XT)	1756-ESMNSE(XT) 1756-SPESMNSE(XT)
20 °C	12	12	0
40 °C	10	10	0
60 °C	7	7	0

Gestione del firmware con Firmware Supervisor

Per gestire il firmware sui controllori, è possibile usare la funzione Firmware Supervisor. Firmware Supervisor consente ai controllori di aggiornare automaticamente i dispositivi:

- I moduli locale e remoto possono essere aggiornati mentre si trovano in modalità Programmazione o Esecuzione.
- La codifica elettronica deve essere configurata per la corrispondenza esatta.
- Il kit del firmware per il dispositivo di destinazione deve risiedere nella scheda di memoria del controllore.
- Il dispositivo deve supportare l'aggiornamento del firmware tramite il software ControlFLASH.

Firmware Supervisor supporta prodotti I/O distribuiti non modulari installati direttamente sulla rete senza adattatori, ivi compresi i dispositivi I/O di sicurezza installati su reti EtherNet/IP. I dispositivi I/O di sicurezza su reti DeviceNet e i moduli POINT Guard I/O non sono ancora supportati.

Per abilitare Firmware Supervisor, attenersi alla seguente procedura.

1. Dalla finestra di dialogo Controller Properties, fare clic sulla scheda Nonvolatile Memory.
2. Fare clic su Load/Store.
3. Dal menu a tendina Automatic Firmware Updates, selezionare Enable e Store Files to Image.

L'applicazione Logix Designer trasferisce i kit del firmware dal computer alla scheda di memoria del controllore affinché possano essere utilizzati da Firmware Supervisor.

SUGGERIMENTO Disabilitando Firmware Supervisor, si disabilitano soltanto gli aggiornamenti del firmware tramite Supervisor. Ciò non riguarda gli aggiornamenti del firmware del controllore che vengono eseguiti quando l'immagine del controllore viene ricaricata dalla scheda di memoria.

Monitoraggio dello stato e gestione degli errori

Argomento	Pagina
Visualizzazione dello stato attraverso la barra online	119
Monitoraggio delle connessioni	120
Monitoraggio degli indicatori di stato	121
Monitoraggio dello stato di sicurezza	122
Errori del controllore	122
Sviluppo di una routine di errore	124

Per informazioni sull'interpretazione degli indicatori di stato e dei messaggi del display controllore, vedere l'Appendice A, Indicatori di stato.

Visualizzazione dello stato attraverso la barra online

Nella barra online sono visualizzate le informazioni sul progetto e sul controllore, compresi lo stato del controllore, lo stato delle forzature, lo stato di modifica online e lo stato di sicurezza.

Figura 32 – Pulsanti di stato

Quando è selezionato il pulsante di stato del controllore come mostrato sopra, la barra online visualizza la modalità (RUN) e lo stato (OK) del controllore. L'indicatore BAT mostra lo stato sia del controllore primario sia del coprocessore di sicurezza. Se entrambi o uno dei due dispositivi presentano un errore della batteria, l'indicatore di stato si illumina. L'indicatore I/O mostra lo stato sia dell'I/O standard sia quello di sicurezza e funziona esattamente come l'indicatore di stato sul controllore. L'I/O con lo stato d'errore più significativo viene visualizzato accanto all'indicatore di stato.

Quando è selezionato il pulsante Stato di sicurezza come mostrato di seguito, la barra online visualizza la firma del task di sicurezza.

Figura 33 – Visualizzazione online della firma di sicurezza

Il pulsante Safety Status indica se il controllore è in blocco o sblocco di sicurezza oppure se presenta un errore. Viene inoltre visualizzata un'icona indicante lo stato di sicurezza.

Tabella 39 - Icona dello stato di sicurezza

Se lo stato di sicurezza è	Viene visualizzata l'icona
Task di sicurezza OK	
Task di sicurezza non funzionante	
Coprocessore di sicurezza mancante Coprocessore di sicurezza non disponibile Hardware non compatibile Firmware non compatibile	
Offline	

Le icone sono verdi quando il controllore è in blocco di sicurezza, gialle quando il controllore non è in blocco di sicurezza e rosse quando il controllore presenta un errore di sicurezza. Se è presente una firma del task di sicurezza, l'icona include un piccolo segno di spunta.

Monitoraggio delle connessioni

È possibile monitorare lo stato delle connessioni standard e di sicurezza.

Tutte le connessioni

Se la comunicazione con un dispositivo nella configurazione I/O del controllore non avviene entro 100 ms, si verifica un timeout della comunicazione ed il controllore genera i seguenti avvisi:

- L'indicatore I/O sulla parte anteriore del controllore lampeggia in verde.
- Viene mostrato un simbolo di avviso ⚠ sulla cartella di configurazione I/O e sul dispositivo in cui si è verificato il timeout.
- Viene generato un errore del dispositivo a cui si può accedere attraverso la scheda Connections della finestra di dialogo Module Properties del dispositivo o attraverso l'istruzione GSV.

ATTENZIONE: Gli I/O di sicurezza e le connessioni prodotte e consumate non possono essere configurate per generare automaticamente un errore del controllore quando la connessione viene interrotta. Pertanto, occorre monitorare gli errori di connessione per accertarsi che il sistema di sicurezza mantenga l'integrità SIL 3/PLe.

Vedere Connessioni di sicurezza a pagina 121.

Connessioni di sicurezza

Per i tag associati ai dati di sicurezza prodotti o consumati, è possibile monitorare lo stato delle connessioni di sicurezza utilizzando il membro CONNECTION_STATUS. Per monitorare le connessioni di ingresso e uscita, i tag I/O di sicurezza dispongono di un membro per lo stato di connessione denominato SafetyStatus. Entrambi i tipi di dati contengono due bit: RunMode e ConnectionFaulted.

Il valore RunMode indica se i dati consumati vengono aggiornati attivamente da un dispositivo che si trova in modalità Run (1) o in stato Idle (0). Lo stato di riposo è indicato se la connessione è chiusa, si è verificato un errore del task di sicurezza o il controllore remoto oppure il dispositivo è in modalità programmazione o test.

Il valore ConnectionFaulted indica se la connessione di sicurezza tra il produttore di sicurezza e il consumatore di sicurezza è Valid (0) o Faulted (1). Se ConnectionFaulted viene impostato su Faulted (1) a seguito della perdita della connessione fisica, i dati di sicurezza vengono azzerati.

Nella seguente tabella sono descritte le combinazioni degli stati RunMode e ConnectionFaulted.

Tabella 40 - Stato delle connessioni di sicurezza

Stato RunMode	Stato ConnectionFaulted	Funzionamento della connessione di sicurezza
1 = Run	0 = Valid	I dati vengono controllati attivamente dal dispositivo produttore, che si trova in modalità Esecuzione.
0 = Idle	0 = Valid	La connessione è attiva e il dispositivo produttore si trova nello stato di riposo. I dati di sicurezza vengono azzerati.
0 = Idle	1 = Faulted	La connessione di sicurezza è in errore. Lo stato del dispositivo produttore è sconosciuto. I dati di sicurezza vengono azzerati.
1 = Run	1 = Faulted	Stato non valido.

Se il dispositivo è inibito, il bit ConnectionFaulted viene impostato su Faulted (1) ed il bit RunMode viene impostato su Idle (0) per ciascuna connessione associata al dispositivo. Di conseguenza, i dati di sicurezza consumati vengono azzerati.

Monitoraggio degli indicatori di stato

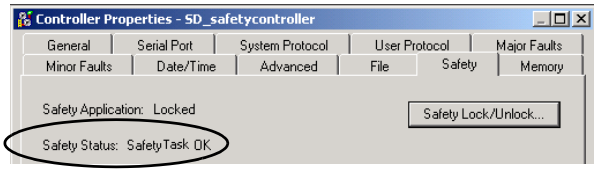
Tutti i controllori Logix, inclusi i GuardLogix, supportano le keyword di stato utilizzabili nella logica per monitorare determinati eventi specifici.

Per ulteriori informazioni sull'utilizzo delle keyword, consultare Logix5000 Controllers Controller Information and Status Programming Manual, pubblicazione 1756-PM015.

Monitoraggio dello stato di sicurezza

Per visualizzare informazioni relative allo stato di sicurezza del controllore, utilizzare il pulsante di stato di sicurezza sulla barra online e nella scheda Safety nella finestra di dialogo Controller Properties.

Figura 34 – Stato del task di sicurezza



I valori possibili per lo stato di sicurezza sono:

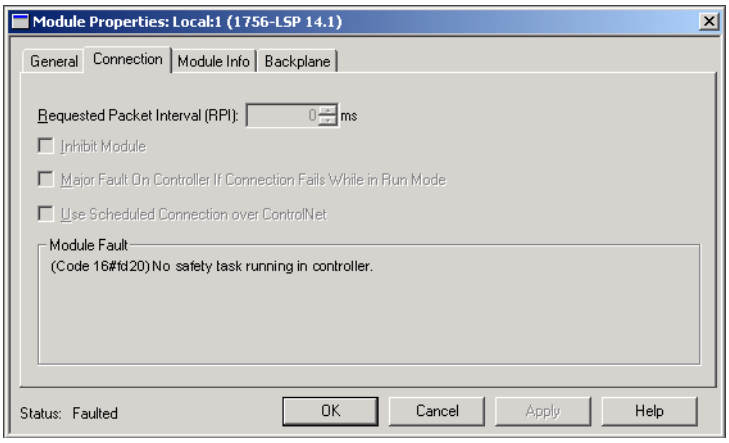
- Coprocessore di sicurezza mancante o non disponibile.
- Hardware del coprocessore di sicurezza non compatibile con il controllore primario.
- Firmware del coprocessore di sicurezza non compatibile con il controllore primario.
- Task di sicurezza non funzionante.
- Task di sicurezza funzionante.

Ad eccezione dell'ultima, le descrizioni riportate sopra indicano che sono presenti errori di sicurezza irreversibili.

Per informazioni sui codici di errore e le misure correttive, vedere Errori gravi di sicurezza (Tipo 14) a pagina 124.

Lo stato del coprocessore di sicurezza può essere visualizzato nella scheda Connections della finestra di dialogo Module Properties.

Figura 35 – Stato del coprocessore di sicurezza



Errori del controllore

Gli errori all'interno del sistema GuardLogix possono essere errori del controllore irreversibili, errori di sicurezza irreversibili nell'applicazione di sicurezza oppure errori di sicurezza reversibili nell'applicazione di sicurezza.

Errori irreversibili del controllore

Questi errori si verificano quando la diagnostica interna del controllore non funziona. Se si verifica un errore irreversibile del controllore, l'esecuzione del task di sicurezza si interrompe e i dispositivi I/O di sicurezza passano allo stato di sicurezza. Per il ripristino è necessario scaricare nuovamente il programma applicativo.

Errori di sicurezza irreversibili nell'applicazione di sicurezza

Se si verifica un errore di sicurezza irreversibile in un'applicazione di sicurezza, la logica di sicurezza e il protocollo di sicurezza vengono interrotti. Gli errori del watchdog del task di sicurezza e dell'associazione di controllo rientrano in questa categoria.

Se si verifica un errore di sicurezza irreversibile del task di sicurezza che viene azzerato dal programma nel gestore degli errori del controllore, l'esecuzione dell'applicazione standard non viene interrotta.

ATTENZIONE: L'esclusione dell'errore di sicurezza non lo azzera. Chi esclude l'errore di sicurezza deve dimostrare che tale operazione non compromette un funzionamento sicuro del sistema.

È necessario fornire prova all'agenzia di certificazione che il sistema può continuare a funzionare in sicurezza anche escludendo un errore di sicurezza.

Se è presente una firma del task di sicurezza, è possibile azzerare l'errore per consentire l'esecuzione del task di sicurezza. Se la firma del task di sicurezza non è stata configurata, il task di sicurezza non può continuare ad essere eseguito finché non viene nuovamente scaricata l'intera applicazione.

Errori reversibili nell'applicazione di sicurezza

Se nell'applicazione di sicurezza si verificano errori reversibili, il sistema potrebbe interrompere l'esecuzione del task di sicurezza, a seconda che l'errore venga gestito o meno dal gestore degli errori del programma nell'applicazione di sicurezza.

Se un errore reversibile viene azzerato da programma, il task di sicurezza continua senza interruzioni.

Se un errore reversibile nell'applicazione di sicurezza non viene azzerato da programma, si verifica un errore di sicurezza reversibile di tipo 14, codice 2. L'esecuzione del programma di sicurezza viene interrotta e le connessioni del protocollo di sicurezza vengono chiuse e riaperte per la reinizializzazione. Le uscite di sicurezza vengono impostate nello stato di sicurezza e il produttore dei tag di sicurezza consumati comanda ai consumatori di impostarle in uno stato di sicurezza.

Gli errori reversibili consentono di modificare l'applicazione standard e di sicurezza in modo tale da correggere la causa dell'errore. Tuttavia, se è stata configurata una firma del task di sicurezza o il controllore è in blocco di sicurezza, è necessario sbloccarlo ed eliminare la firma del task di sicurezza prima di poter modificare l'applicazione di sicurezza.

Visualizzazione degli errori

La finestra di dialogo Recent Faults sulla scheda Major Faults della finestra di dialogo Controller Properties contiene altre due schede, una per gli errori standard e l'altra per gli errori di sicurezza.

Anche il display di stato del controllore visualizza i codici di errore accompagnati da un breve messaggio di stato, come spiegato all'inizio di pagina 127.

Codici di errore

La Tabella 41 mostra i codici di errore specifici dei controllori GuardLogix. Il tipo e il codice corrispondono al tipo e al codice visualizzati nella scheda Major Faults della finestra di dialogo ControllerProperties e nell'oggetto PROGRAM, attributo MAJORFAULTRECORD (o MINORFAULTRECORD).

Tabella 41 - Errori gravi di sicurezza (Tipo 14)

Codice	Causa	Stato	Azione correttiva
01	Watchdog del task scaduto. Il task utente non è stato completato in un periodo di tempo specificato. Un errore di programma ha causato un loop infinito, il programma è troppo complesso per essere eseguito nei tempi specificati, un task con priorità più alta impedisce il completamento di questo task, oppure il coprocessore di sicurezza è stato rimosso.	Irreversibile	Rimuovere l'errore. Se è presente una firma del task di sicurezza, la memoria di sicurezza viene reinizializzata e viene avviata l'esecuzione del task di sicurezza. Se non è presente una firma del task di sicurezza, è necessario scaricare nuovamente il programma per consentire l'esecuzione del task di sicurezza. Installare il coprocessore di sicurezza, se è stato rimosso.
02	È presente un errore in una routine del task di sicurezza.	Reversibile	Correggere l'errore nella logica del programma utente.
03	Il coprocessore di sicurezza è mancante.	Irreversibile	Installare un coprocessore di sicurezza compatibile.
04	Il coprocessore di sicurezza non è disponibile.	Irreversibile	Installare un coprocessore di sicurezza compatibile.
05	L'hardware del coprocessore di sicurezza non è compatibile.	Irreversibile	Installare un coprocessore di sicurezza compatibile.
06	Il firmware del coprocessore di sicurezza non è compatibile.	Irreversibile	Aggiornare il coprocessore di sicurezza, in modo che le versioni principale e secondaria del firmware corrispondano al controllore primario.
07	Task di sicurezza non funzionante. Questo errore si verifica quando la logica di sicurezza non è valida, ad esempio in caso di mancata corrispondenza nella logica tra il controllore primario e il coprocessore di sicurezza, se si verifica un timeout del watchdog, oppure se la memoria è danneggiata.	Irreversibile	Rimuovere l'errore. Se è presente una firma del task di sicurezza, la memoria di sicurezza viene reinizializzata tramite la firma del task di sicurezza e viene avviata l'esecuzione del task di sicurezza. Se non è presente una firma del task di sicurezza, è necessario scaricare nuovamente il programma per consentire l'esecuzione del task di sicurezza.
08	Tempo di sistema coordinato (CST) non trovato.	Irreversibile	Rimuovere l'errore. Configurare un dispositivo come master CST.
09	Errore irreversibile del coprocessore di sicurezza.	Irreversibile	Rimuovere l'errore e scaricare il programma. Se il problema persiste, sostituire il coprocessore di sicurezza.

Logix5000 Controllers Major and Minor Faults Programming Manual, pubblicazione 1756-PM014 contiene informazioni dettagliate relative ai codici di errore comuni ai controllori Logix.

Sviluppo di una routine di errore

Se si verifica una condizione d'errore sufficientemente grave da determinare lo spegnimento del controllore, quest'ultimo genera un errore grave ed arresta l'esecuzione della logica.

Per alcune applicazioni non è necessario che tutti gli errori di sicurezza arrestino l'intero sistema. In queste situazioni, è possibile utilizzare una routine di errore per rimuovere un errore specifico e far continuare a funzionare la parte di controllo standard del sistema oppure configurare alcune uscite perché rimangano attive.

ATTENZIONE: È necessario fornire prova all'agenzia di certificazione che il sistema può continuare a funzionare in sicurezza anche escludendo un errore di sicurezza.

Il controllore supporta due livelli per la gestione degli errori gravi:

- Routine di errore del programma
- Gestore degli errori del controllore

Entrambe le routine possono utilizzare le istruzioni GSV e SSV, come descritto a pagina 125.

Routine di errore del programma

Ciascun programma può avere una propria routine di errore. Il controllore esegue la routine di errore del programma quando si verifica un errore dell'istruzione. Se la routine di errore del programma non consente di rimuovere l'errore oppure la routine di errore del programma non esiste, il controllore procede all'esecuzione del gestore degli errori del controllore, se presente.

Gestore degli errori del controllore

Il gestore degli errori del controllore è un componente opzionale eseguito quando la routine di errore del programma non è in grado di rimuovere l'errore o non esiste.

È possibile creare un programma per il gestore degli errori del controllore. Dopo avere creato il programma, è necessario configurare una routine come routine principale.

Per informazioni dettagliate sulla creazione e il test di una routine di errore, consultare Logix5000 Controllers Major and Minor Faults Programming Manual, pubblicazione 1756-PM014.

Utilizzo delle istruzioni GSV/SSV

I controllori Logix memorizzano i dati di sistema in oggetti anzichè in file di stato. È possibile utilizzare le istruzioni Get System Value (GSV) e Set System Value (SSV) per leggere e scrivere i dati del controllore.

L'istruzione GSV recupera le informazioni specificate e le posiziona in una destinazione specifica. L'istruzione SSV cambia l'attributo specifico con i dati dall'origine dell'istruzione. Per un'istruzione GSV o SSV, il software di programmazione visualizza le classi degli oggetti, i nomi degli oggetti e i nomi degli attributi per ciascuna istruzione.

Per i task standard, è possibile utilizzare l'istruzione GSV per ottenere i valori degli attributi disponibili. Quando si utilizza l'istruzione SSV, il software visualizza solo gli attributi configurabili dall'utente.

Per il task di sicurezza, le istruzioni GSV e SSV sono più limitate. Si noti che le istruzioni SSV nei task di sicurezza e in quelli standard non possono impostare il bit 0 (errore grave in caso di errore) nell'attributo della modalità di un dispositivo I/O di sicurezza.

Per gli oggetti di sicurezza, la Tabella 42 riporta gli attributi per i quali è possibile ottenere valori utilizzando l'istruzione GSV e quelli che è possibile impostare tramite l'istruzione SSV, nei task sia standard sia di sicurezza.

ATTENZIONE: Utilizzare le istruzioni GSV/SSV con molta attenzione. La modifica degli oggetti può causare operazioni del controllore non previste o infortuni al personale.

Tabella 42 - Accessibilità di GSV/SSV

Oggetto di sicurezza	Nome attributo	Tipo di dati	Descrizione attributo	Accessibile dal task di sicurezza		Accessibile dai task standard	
				GSV	SSV	GSV[4]	SSV
Task di sicurezza	Instance	DINT	Fornisce il numero di istanza di questo oggetto del task. I valori validi sono compresi tra 0 e 31.	X		X	
	MaximumInterval	DINT[2]	L'intervallo di tempo massimo tra le esecuzioni successive del task.			X	X
	MaximumScanTime	DINT	Il tempo di esecuzione massimo registrato (ms) per il task.			X	X
	MinimumInterval	DINT[2]	L'intervallo di tempo minimo tra le esecuzioni successive del task.			X	X
	Priority	INT	Priorità relativa di questo task rispetto ad altri task. I valori validi sono compresi tra 0 e 15.	X		X	
	Rate	DINT	Periodo del task (in ms) o valore di timeout per il task (in ms).	X		X	
	Watchdog	DINT	Limite di tempo (in ms) per l'esecuzione di tutti i programmi associati al task.	X		X	
Programma di sicurezza	Instance	DINT	Fornisce il numero di istanza dell'oggetto del programma.	X		X	
	MajorFaultRecord[1]	DINT[11]	Registra gli errori gravi per il programma.	X	X	X	
	MaximumScanTime	DINT	Il tempo di esecuzione massimo registrato (ms) per il programma.			X	X
Routine di sicurezza	Instance	DINT	Fornisce il numero di istanza di questo oggetto di routine. I valori validi sono compresi tra 0 e 65.535.	X			
Controllore di sicurezza	SafetyLocked	SINT	Indica se il controllore è in blocco o sblocco di sicurezza.	X		X	
	SafetyStatus[2]	INT	Specifica lo stato di sicurezza come: • Task di sicurezza funzionante. (1000000000000000) • Task di sicurezza non funzionante. (1000000000000001) • Coprocessore mancante. (00000000000000000) • Coprocessore non disponibile (00000000000000001) • Hardware non compatibile (00000000000000010) • Firmware non compatibile (00000000000000011)			X	
	SafetySignatureExists	SINT	Indica se la firma del task di sicurezza è presente.	X		X	
	SafetySignatureID	DINT	Numero identificativo a 32 bit.			X	
	SafetySignature	Stringa[3]	Numero identificativo a 32 bit.			X	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Registra gli errori del task di sicurezza.			X	
AOI (sicurezza)	LastEditDate	LINT	Registrazione cronologica di data ed ora dell'ultima modifica apportata alla definizione di un'istruzione Add-On.			X	
	SignatureID	DINT	Numero ID.			X	
	SafetySignatureID	DINT	Numero identificativo a 32 bit.			X	

(1) Per ulteriori informazioni su come accedere a questo attributo, vedere Accesso agli attributi FaultRecord a pagina 127.

(2) Per ulteriori informazioni su come accedere a questo attributo, vedere Acquisizione di informazioni sugli errori a pagina 127.

(3) Lunghezza = 37.

(4) Dal task standard, l'accessibilità GSV degli attributi dell'oggetto di sicurezza è la stessa degli attributi dell'oggetto standard.

Accesso agli attributi FaultRecord

Per semplificare l'accesso agli attributi MajorFaultRecord e SafetyTaskFaultRecord occorre creare una struttura definita dall'utente.

Tabella 43 - Parametri di accesso agli attributi FaultRecord

Nome	Tipo di dati	Stile	Descrizione
TimeLow	DINT	Decimale	32 bit inferiori del valore di registrazione ora e data dell'errore
TimeHigh	DINT	Decimale	32 bit superiori del valore di registrazione ora e data dell'errore
Type	INT	Decimale	Tipo di errore (programma, I/O o altro)
Code	INT	Decimale	Codice univoco per questo errore (dipendente dal tipo di errore)
Info	DINT[8]	Esadecimale	Informazioni specifiche sull'errore (dipendenti dal tipo di errore e dal codice)

Per ulteriori informazioni sull'utilizzo delle istruzioni GSV e SSV, consultare il capitolo dedicato alle istruzioni di ingresso/uscita del manuale di riferimento Istruzioni generali per controllori Logix5000, pubblicazione 1756-RM003K-IT-P.

Acquisizione di informazioni sugli errori

Gli attributi SafetyStatus e SafetyTaskFaultRecord consentono di acquisire informazioni relative agli errori irreversibili. Per acquisire e memorizzare le informative relative agli errori si utilizza un'istruzione GSV nel gestore degli errori del controllore. L'istruzione GSV può essere utilizzata in un task standard insieme ad una routine del gestore degli errori del controllore che azzera l'errore e permette il proseguimento dell'esecuzione dei task standard.

Note:

Indicatori di stato

Argomento	Pagina
Indicatori di stato dei controllori	129
Display dello stato del controllore	130

Indicatori di stato dei controllori

Lo stato del controllore primario viene visualizzato tramite quattro indicatori di stato.

Tabella 44 - Descrizioni degli indicatori di stato del controllore primario

Indicatore	Stato	Descrizione
RUN	Spento	Nessuna attività utente in esecuzione. Il controllore è in modalità PROGram.
	Verde	Il controllore è in modalità RUN.
FORCE	Spento	Nessuna forzatura, standard o di sicurezza, è abilitata sul controllore.
	Arancione	Le forzature standard e/o di sicurezza sono state abilitate. **Se si installa una forzatura, prestare la massima attenzione. Se si installa una forzatura, questa ha effetto immediato.**
	Arancione, lampeggiante	Uno o più indirizzi I/O, standard e/o di sicurezza, sono stati forzati sullo stato On o Off, ma le forzature non sono state abilitate. **Prestare attenzione durante l'abilitazione delle forzature I/O, perché l'azione coinvolge anche tutte le forzature I/O esistenti.**
SD	Spento	Nessuna attività con la scheda di memoria.
	Verde, lampeggiante	Il controllore sta leggendo o scrivendo sulla scheda di memoria. Non rimuovere la scheda di memoria mentre il controllore sta leggendo o scrivendo.
	Verde	
	Rosso, lampeggiante	La scheda di memoria non presenta un file system valido.
	Rosso	La scheda di memoria non viene riconosciuta dal controllore.
OK	Spento	Nessuna alimentazione applicata.
	Verde	Il controllore è in funzione senza alcun errore.
	Rosso, lampeggiante	• Errore irreversibile o errore reversibile non gestito nel gestore errori. Tutte le attività utente, sia standard che di sicurezza, sono interrotte. • Se il controllore è nuovo, serve un aggiornamento firmware. Il display di stato indica Firmware Installation Required.
	Rosso	• Il controllore sta completando la diagnostica all'accensione. • Si è verificato un errore grave irreversibile e il programma è stato cancellato dalla memoria. • Il condensatore del Modulo di alimentazione (ESM) è in fase di scarica per spegnimento. • Il controllore è acceso, ma non funzionante. • Il controllore sta caricando un progetto nella memoria non volatile.

Il coprocessore di sicurezza presenta un indicatore di stato OK.

Tabella 45 - Indicatore di stato 1756-L7SP

Indicatore	Stato	Descrizione
OK	Spento	Nessuna alimentazione applicata.
	Verde	Il coprocessore di sicurezza è in funzione senza alcun errore.
	Rosso	Errore del controllore all'accensione o errore irreversibile.

Display dello stato del controllore

Il display di stato del controllore visualizza a scorrimento una serie di messaggi che forniscono informazioni su versione firmware del controllore, stato del modulo ESM, stato del progetto ed errori gravi.

Messaggi di stato di sicurezza

Il display del controllore primario può visualizzare i seguenti messaggi. Il coprocessore di sicurezza visualizza "L7SP".

Tabella 46 - Display di stato di sicurezza

Messaggio	Interpretazione
No Safety Signature	Il task di sicurezza è in modalità Esecuzione senza una firma del task di sicurezza.
Safety Partner Missing	Coprocessore di sicurezza mancante o non disponibile.
Hardware Incompatible	Hardware del coprocessore di sicurezza non compatibile con quello del controllore primario.
Firmware Incompatible	Versione firmware del coprocessore di sicurezza non compatibile con quella del controllore primario.
No CST Master	Impossibile trovare un master CST (tempo di sistema coordinato).
Task di sicurezza non funzionante	Logica di sicurezza non valida. Ad esempio, mancata corrispondenza tra il controllore primario e il coprocessore di sicurezza, timeout del watchdog o danneggiamento della memoria.
Safety Unlocked	Il controllore è in modalità Esecuzione con una firma di sicurezza, ma non in blocco di sicurezza.

Messaggi di stato generali

I messaggi descritti nella Tabella 47 vengono generalmente visualizzati all'accensione, allo spegnimento e mentre il controllore è in funzione. Questi messaggi indicano lo stato del controllore e del modulo ESM.

Tabella 47 - Display di stato generale

Messaggio	Interpretazione
Nessun messaggio	Il controllore è spento o si è verificato un errore grave irreversibile (MNRF). Controllare l'indicatore di stato OK per stabilire se il controllore è alimentato e determinarne lo stato.
TEST	Il controllore sta eseguendo le prove previste all'accensione.
PASS	Le prove previste all'accensione hanno avuto risultato positivo.
SAVE	Allo spegnimento, un progetto viene salvato sulla scheda SD. Per ulteriori informazioni di stato, è possibile controllare anche l'indicatore SD (vedere pagina 129). Prima di rimuovere la scheda SD o interrompere l'alimentazione attendere che il salvataggio sia completo.
LOAD	All'accensione del controllore, dalla scheda SD viene caricato un progetto. Per ulteriori informazioni di stato, è possibile controllare anche l'indicatore SD (vedere pagina 129). Prima di rimuovere la scheda SD o il modulo ESM e prima di interrompere l'alimentazione, attendere che il caricamento sia completo.
UPDT	All'accensione, viene eseguito un aggiornamento firmware dalla scheda SD. Per ulteriori informazioni di stato, è possibile controllare anche l'indicatore SD (vedere pagina 129). Se non si desidera l'aggiornamento del firmware all'accensione, modificare l'opzione Load Image del controllore.
CHRG	Il modulo ESM con condensatore è in fase di carica.
1756-L7*x*/*X*	Numero di catalogo e serie del controllore.
Rev *XX.xxx*	Versioni principale e secondaria del firmware per il controllore.
No Project	Nel controllore non è caricato alcun progetto. Per caricare un progetto, usare l'applicazione Logix Designer per scaricare il progetto nel controllore o utilizzare una scheda SD per caricare il progetto nel controllore.
Project Name	Nome del progetto attualmente caricato nel controllore. Il nome indicato è quello specificato come nome del progetto nell'applicazione Logix Designer.
BUSY	I dispositivi I/O associati al controllore non sono ancora pienamente alimentati. Attendere che i dispositivi I/O completino le fasi di accensione e autodiagnostica.
Corrupt Certificate Received	Il certificato di sicurezza associato al firmware è danneggiato. Accedere all'indirizzo http://www.rockwellautomation.com/support/ e scaricare la versione firmware che si desidera aggiornare. Sostituire la versione firmware precedentemente installata con quella disponibile nel sito Web dell'assistenza tecnica.
Corrupt Image Received	Il file del firmware è danneggiato. Accedere all'indirizzo http://www.rockwellautomation.com/support/ e scaricare la versione firmware che si desidera aggiornare. Sostituire la versione firmware precedentemente installata con quella disponibile nel sito Web dell'assistenza tecnica.
ESM Not Present	Manca un modulo ESM e, allo spegnimento, il controllore non può salvare l'applicazione. Inserire un modulo ESM compatibile e, se si utilizza un modulo ESM con condensatore, non interrompere l'alimentazione fino al completo caricamento del modulo ESM.
ESM Incompatible	Il modulo ESM non è compatibile con le dimensioni della memoria del controllore. Sostituire il modulo ESM incompatibile con uno compatibile.
ESM Hardware Failure	Il modulo ESM è in guasto e, in caso di spegnimento, il controllore non può salvare il programma. Sostituire il modulo ESM prima di interrompere l'alimentazione del controllore, in modo da poter salvare il programma.
ESM Energy Low	Il modulo ESM con condensatore non ha energia sufficiente a permettere al controllore di salvare il programma in caso di spegnimento. Sostituire il modulo ESM.
ESM Charging	Il modulo ESM con condensatore è in fase di carica. Non interrompere l'alimentazione fino al completamento della carica.
Flash in Progress	È in corso un aggiornamento firmware avviato mediante ControlFLASH o AutoFlash. Lasciar completare l'aggiornamento firmware senza interruzioni.
Firmware Installation Required	Il controllore sta usando il firmware di avvio (versione 1.*xxx*) e richiede un aggiornamento firmware. Aggiornare il firmware del controllore.
SD Card Locked	La scheda SD installata è bloccata.

Messaggi di errore

Se il controllore è in stato di errore, sul display di stato viene visualizzato uno dei seguenti messaggi.

Tabella 48 - Messaggi di errore(1)

Messaggio	Interpretazione
Major Fault T*XX*:C*XX message*	Rilevamento di un errore grave di Tipo *XX* e Codice *XX*. Ad esempio, se il display di stato visualizza Major Fault T04:C42 Invalid JMP Target, significa che un'istruzione JMP è programmata per passare ad un'istruzione LBL non valida.
I/O Fault Local:*X #XXXX message*	Si è verificato un errore I/O in un modulo dello chassis locale. Vengono indicati il numero di slot e il codice di errore, accompagnati da una breve descrizione. Ad esempio, il messaggio I/O Fault Local:3 #0107 Connection Not Found indica che una connessione al modulo I/O locale nello slot tre non è aperta. Adottare la misura correttiva specifica per il tipo di errore indicato.
I/O Fault *ModuleName #XXXX message*	Si è verificato un errore I/O su un modulo nello chassis remoto. Il nome del modulo in errore, come configurato nell'albero di configurazione I/O dell'applicazione Logix Designer, è accompagnato dal codice di errore e da una breve descrizione. Ad esempio, I/O Fault My_Module #0107 Connection Not Found indica che una connessione al modulo designato come "My_Module" non è aperta. Adottare la misura correttiva specifica per il tipo di errore indicato.
I/O Fault *ModuleParent:X #XXXX message*	Si è verificato un errore I/O su un modulo nello chassis remoto. È indicato il nome del modulo madre perché, nell'albero di configurazione I/O dell'applicazione Logix Designer, non è configurato alcun nome. Inoltre, il codice di errore è accompagnato da una breve descrizione. Ad esempio, I/O Fault My_CNet:3 #0107 Connection Not Found indica che una connessione ad un modulo nello slot 3 dello chassis con il modulo di comunicazione denominato "My_CNet" non è aperta. Adottare la misura correttiva specifica per il tipo di errore indicato.
X I/O Faults	Sono presenti errori I/O e *X* = il numero di errori I/O presenti. In presenza di più errori I/O, il controllore segnala il primo errore registrato. Quando ogni errore I/O è stato risolto, il numero di errori indicato diminuisce e il messaggio di errore I/O indica l'errore successivo. Adottare la misura correttiva specifica per il tipo di errore indicato.

(1) Per i dettagli sui codici di errore, consultare Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, pubblicazione1756-PM014.

Messaggi relativi agli errori gravi reversibili

Gli errori gravi reversibili vengono segnalati dal messaggio Major Fault T*XX*:C*XX* sul display di stato del controllore. La Tabella 49 a pagina 133 elenca i tipi di guasto, i codici e i messaggi associati specifici che vengono visualizzati sul display di stato.

Per le descrizioni dettagliate e i metodi di ripristino suggeriti degli errori gravi reversibili, consultare Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, pubblicazione 1756-PM014.

Tabella 49 - Messaggi di stato degli errori gravi reversibili

Type	Codice	Messaggio
1	1	Run Mode Powerup
1	60	Non-recoverable
1	61	Non-recoverable – Diagnostics Saved
1	62	Non-recoverable – Program Saved
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN or POS < 0
4	31	Invalid JSR Parameter
4	34	Timer Failure
4	42	Invalid JMP Target
4	82	SFC Jump Back Failure
4	83	Value Out of Range
4	84	Stack Overflow
4	89	Invalid Target Step
4	90	Invalid Instruction
4	91	Invalid Context
4	92	Invalid Action
4	990	Definiti dall'utente
4	991	
4	992	
4	993	
4	994	
4	995	
4	996	
4	997	
4	998	
4	999	
6	1	Task Watchdog Expired
7	40	Save Failure

Type	Codice	Messaggio
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
8	1	key switch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	6	SERCOS Drive Fault
11	7	Synchronous Connection Fault
11	8	Servo Module Fault
11	9	Asynchronous Connection Fault
11	10	Motor Fault
11	11	Motor Thermal Fault
11	12	Drive Thermal Fault
11	13	SERCOS Communications Fault
11	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	Drive Guard Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

Codici di errore I/O

Gli errori I/O segnalati dal controllore vengono visualizzati sul display di stato in uno dei seguenti formati:

- I/O Fault Local:*X #XXXX message*
- I/O Fault *ModuleName #XXXX message*
- I/O Fault *ModuleParent*:*X #XXXX message*

La prima parte del formato indica la posizione del modulo in errore. Il modo in cui la posizione viene indicata dipende dalla configurazione I/O e dalle proprietà dei moduli specificate nell'applicazione Logix Designer.

L'ultima parte del formato, #XXXX message, può essere utilizzata per diagnosticare il tipo di errore I/O e le possibili misure correttive. Per i dettagli su ogni codice di errore I/O, consultare Logix5000 Major, Minor, and I/O Fault Codes Programming Manual, pubblicazione 1756-PM014.

Tabella 50 - Messaggi di errore I/O

Codice	Messaggio
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax
#0005	Destination Unknown
#0006	Partial Data Transferred
#0007	Connection Lost
#0008	Service Unsupported
#0009	Invalid Attribute Value
#000A	Attribute List Error
#000B	State Already Exists
#000C	Object Mode Conflict
#000D	Object Already Exists
#000E	Attribute Not Settable
#000F	Permission Denied
#0010	Device State Conflict
#0011	Reply Too Large
#0012	Fragment Primitive
#0013	Insufficient Command Data
#0014	Attribute Not Supported
#0015	Data Too Large
#0100	Connection In Use
#0103	Transport Not Supported
#0106	Ownership Conflict
#0107	Connection Not Found
#0108	Invalid Connection Type
#0109	Invalid Connection Size
#0110	Module Not Configured
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module

Codice	Messaggio
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#0304	ControlNet Schedule Error
#0305	Signature Mismatch
#0306	CCM Not Available
#0311	Invalid Port
#0312	Invalid Link Address
#0315	Invalid Segment Type
#0317	Connection Not Scheduled
#0318	Invalid Link Address
#0319	No Secondary Resources Available
#031E	No Available Resources
#031F	No Available Resources
#0800	Network Link Offline
#0801	Incompatible Multicast RPI
#0802	Invld Safety Conn Size
#0803	Invld Safety Conn Format
#0804	Invld Time Correct Conn Format
#0805	Invld Ping Intrvl EPI Multiplier
#0806	Time Coord Msg Min Multiplier

Messaggi di errore I/O (continua)

Codice	Messaggio
#0807	Time Expectation Multiplier
#0808	Timeout Multiplier
#0809	Invld Max Consumer Number
#080A	Invld CPCRC
#080B	Time Correction Conn ID Invld
#080C	Safety Cfg Signature Mismatch
#080D	Safety Netwk Num Not Set OutOfBx
#080E	Safety Netwk Number Mismatch
#080F	Cfg Operation Not Allowed
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD06	SERCOS Transition Fault
#FD07	SERCOS Init Ring Fault
#FD08	SERCOS Comm Fault
#FD09	SERCOS Init Node Fault
#FD0A	Axis Attribute Reject
#FD1F	Safety Data Fault
#FD20	No Safety Task Running
#FD21	Invld Safety Conn Parameter
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection

Codice	Messaggio
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled P/C Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed – Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
—	

Note:

Modifica del tipo di controllore

Argomento	Pagina
Cambio da controllore standard a controllore di sicurezza	137
Cambio da controllore di sicurezza a controllore standard	138
Cambio del tipo di controllore di sicurezza	138
Altre risorse	139

Poiché i controllori di sicurezza hanno requisiti speciali e non supportano determinate funzioni standard, è necessario comprendere il comportamento del sistema durante la modifica del tipo di controllore (da controllore standard a controllore di sicurezza o viceversa) nel progetto del controllore. Il cambio del controllore influisce su quanto segue:

- Funzioni supportate
- Configurazione fisica del progetto (coprocessore di sicurezza e I/O di sicurezza)
- Proprietà del controllore
- Componenti del progetto, quali task, programmi, routine e tag
- Istruzioni Add-On di sicurezza

IMPORTANTE In Studio 5000 versione 21 o successiva, i controllori GuardLogix 5560 e Compact GuardLogix® 1768 non sono supportati.

Cambio da controllore standard a controllore di sicurezza

Per cambiare correttamente il tipo di controllore, passando da un controllore standard ad uno di sicurezza, lo slot dello chassis immediatamente alla destra del controllore primario di sicurezza deve essere disponibile per il coprocessore di sicurezza.

Dopo la conferma del cambiamento del progetto da controllore standard a controllore di sicurezza, vengono creati i componenti di sicurezza per soddisfare i requisiti minimi del controllore di sicurezza:

- Il task di sicurezza viene creato solo se il numero massimo di task scaricabili non è stato raggiunto. Il task di sicurezza viene inizializzato con i valori predefiniti.
- Vengono creati i componenti di sicurezza (ossia task di sicurezza, programma di sicurezza e così via).
- Viene generato un numero di rete di sicurezza (SNN), basato su data e ora, per lo chassis locale.
- Le eventuali funzioni del controllore standard non supportate dal controllore di sicurezza, ad esempio la ridondanza, vengono rimosse dalla finestra di dialogo Controller Properties (se presenti).

Cambio da controllore di sicurezza a controllore standard

Dopo la conferma del cambiamento del progetto da controllore di sicurezza a controllore standard, alcuni componenti vengono modificati ed altri eliminati, come descritto di seguito:

- Il coprocessore di sicurezza viene eliminato dallo chassis I/O.
- I dispositivi I/O di sicurezza e i relativi tag vengono eliminati.
- Task, programmi e routine di sicurezza vengono cambiati in task, programmi e routine standard.
- Tutti i tag di sicurezza, ad eccezione dei tag consumati, vengono cambiati in tag standard. I tag di sicurezza consumati vengono eliminati.
- Le mappature dei tag di sicurezza vengono eliminate.
- Il numero della rete di sicurezza (SNN) viene eliminato.
- Le password di blocco e sblocco di sicurezza vengono eliminate.
- Se il controllore standard supporta funzioni che non erano disponibili con il controllore di sicurezza, queste nuove funzioni risulteranno visibili nella finestra di dialogo Controller Properties.

  SUGGERIMENTO I controllori di sicurezza peer non vengono eliminati, anche se non è rimasta alcuna connessione.

- Le istruzioni potrebbero ancora fare riferimento a moduli che sono stati cancellati e pertanto determinare errori durante le verifiche.
- I tag consumati vengono cancellati quando si elimina il modulo che li ha prodotti.
- A seguito dei cambiamenti nel sistema descritti sopra, le istruzioni di sicurezza e i tag I/O di sicurezza non vengono verificati.

Se il progetto del controllore di sicurezza contiene istruzioni Add-On di sicurezza, è necessario rimuoverle dal progetto o cambiarne la classe in standard prima di cambiare tipo di controllore.

Cambio del tipo di controllore di sicurezza

IMPORTANTE I controllori Compact GuardLogix 1768 e GuardLogix 5560 non sono supportati nell'applicazione Logix Designer, versione 21.

Quando si cambia tipo di controllore di sicurezza, la classe dei tag, delle routine e dei programmi non viene modificata. Gli eventuali dispositivi I/O non più compatibili con il controllore di destinazione vengono eliminati.

La rappresentazione del coprocessore di sicurezza viene aggiornata affinché quest'ultimo sia visualizzato correttamente sul controllore di destinazione:

- Quando si passa da un controllore Compact GuardLogix 1768 a un controllore GuardLogix 5570, il coprocessore di sicurezza viene creato nello slot *x* (slot primario + 1).
- Quando si passa a un controllore Compact GuardLogix 1768, il coprocessore di sicurezza viene rimosso poiché è interno al controllore Compact GuardLogix.

SUGGERIMENTO Il controllore GuardLogix 5570 supporta 100 programmi di sicurezza nel task di sicurezza, mentre il controllore Compact GuardLogix 1768 ne supporta 32.

Le istruzioni a virgola mobile – come FAL, FLL, FSC, SIZE, CMP, SWPB e CPT – sono supportate nei controllori GuardLogix 5570, ma non nei controllori GuardLogix 5560 e Compact GuardLogix 1768. Se il programma di sicurezza contiene queste istruzioni, verranno generati errori di verifica al passaggio da un controllore GuardLogix 5570 ad un controllore GuardLogix 5560 o Compact GuardLogix 1768.

Altre risorse

Per ulteriori informazioni sulle istruzioni Add-On, consultare Logix5000 Controllers Add-On Instructions Programming Manual, pubblicazione 1756-PM010.

Note:

Caratteri numerici

1756-Axx 25
1756-CN2 58
1756-CN2R 58
1756-CN2RXT 58
1756-CNB 58
1756-CNBR 58
1756-DNB 60, 61, 105
1756-EN2F 53
1756-EN2T 53
1756-EN2TR 53
1756-EN2TRXT 53
1756-EN2TXT 53
1756-EN3TR 53
1756-ENBT 53
1756-ESMCAP 24, 34, 36, 116, 118
1756-ESMCAPXT 24, 34, 36, 116, 118
1756-ESMNRM 24, 35, 36, 116, 118
1756-ESMNRMXT 24, 36, 116, 118
1756-ESMNSE 24, 35, 36, 116, 118
1756-ESMNSEXT 24, 36, 116, 118
1756-EWEB 53
1756-PA72 25
1756-PA75 25
1756-PAXT 25
1756-PB72 25
1756-PB75 25
1756-PBXT 25
1756-SPESMCAP 24, 34
1756-SPESMNRM 24, 36, 116
1756-SPESMNRMXT 24, 36, 116
1756-SPESMNSE 24, 35, 36, 116
1756-SPESMNSEXT 24, 34, 36, 116
1784-SD1 24
1784-SD2 24

A

accesso esterno 88, 92
aggiornamenti automatici del firmware 118
aggiornamento
  firmware 31, 32
alimentatore
  numeri di catalogo 17, 25
ambiente 21
ambiente estremo
  alimentatore 25
  chassis 25
  componenti del sistema 10
  controllore 10
approvazione per l'uso in aree pericolose
  Europa 23
  Nord America 22
attributi
  oggetto di sicurezza 125
autenticazione di configurazione
  componenti 71
  copia 71
  definizione 71
AutoFlash
  aggiornamento firmware 32
autonomia
  modulo di alimentazione 118

B

barra online 119
batteria
  errore 119
bit ConnectionFaulted 121
bit RunMode 121
blocco di sicurezza 100
  controllore 101
  effetto sul download 108
  effetto sull'upload 107
  icona 101
  password 101

C

cambio del controllore 138
cancellazione
  errori 123
  programma 117
capacità RAM 16
caricamento di un progetto 115
  all'accensione 115
  avviato dall'utente 115
  se la memoria è danneggiata 115
chassis 17
  numeri di catalogo 25
CIP Safety 11, 47, 80
classe 91
codici di errore
  display di stato 123
  errori gravi di sicurezza 124
  messaggi I/O 134
codifica elettronica 118
collegamento online 111
  fattori 106
componenti del sistema Logix-XT
  vedere ambiente estremo.
comunicazione 18
  moduli 18
  rete ControlNet 58
  rete DeviceNet 60
  rete EtherNet/IP 53
condizioni predefinite in fabbrica 77
  reset modulo 75
configurazione avanzata del tempo di risposta della connessione 69
configure always 80
  casella di controllo 44

CONNECTION_STATUS 93, 121
connessione
monitoraggio 120
non schedulata 59
rete ControlNet 59
rete EtherNet/IP 54
schedulata 59
stato 121
USB 29
connessione di solo ascolto 71
connessioni non schedulate 59
connessioni schedulate 59
consumo dati tag 96
controller
properties 41
controllore
ambiente estremo 10
cambio del tipo 137-139
configurazione 39
corrispondenza 106
funzioni differenti 9
gestore degli errori 125
installazione 25
mancata corrispondenza numero seriale 109, 112
modalità 33
modalità operativa 33, 34
numero seriale 106
registrazione
blocco/sblocco sicurezza 101
firma del task di sicurezza 102
controllore Compact GuardLogix 138
controllore Compact GuardLogix 1768 138
controllore di sicurezza peer
condivisione dati 93
configurazione 45
posizione 93
SNN 93
controllore primario
descrizione 16
memoria utente 16
modalità 16
panoramica dell'hardware 16
controllori GuardLogix
differenze 9
ControlNet
configurazione del driver 106
connessioni 59, 106
esempio 59
moduli di comunicazione 18
modulo 58, 105
non schedulata 59
panoramica 58
schedulata 59
software 58
copertura diagnostica 11
copia
firma del task di sicurezza 103
numero di rete di sicurezza 52
coprocessore di sicurezza
configurazione 17
descrizione 17
stato 122
corrispondenza tra progetto e controllore 106
creazione di un progetto 39
custodia 21

D

dati standard in una routine di sicurezza 98
DeviceNet
comunicazione 60
configurazione del driver 106
connessioni 61, 106
modulo 105
software 60
dispositivi di interfaccia operatore 14
download
effetto del blocco di sicurezza 108
effetto della corrispondenza del controllore 106
effetto della corrispondenza della versione del firmware 107
effetto della firma del task di sicurezza 108
effetto dello stato di sicurezza 107
processo 108-109
driver
ControlNet 106
DeviceNet 106
EtherNet/IP 106
USB 30

E

eliminazione
firma del task di sicurezza 103
errore
cancellazione 123
irreversibile controllore 122
messaggi 132, 133
reversibile 123, 133
routine 124-126
sicurezza irreversibile 122, 123
errore di sicurezza irreversibile 122, 123
riavvio del task di sicurezza 123
errore irreversibile controllore 122
errore reversibile 123, 133
cancellazione 123
errori di verifica
cambio del tipo di controllore 139
errori gravi di sicurezza 124
errori gravi reversibili 133
ESM
Vedere modulo di alimentazione
vedere modulo di alimentazione
EtherNet/IP
capacità modulo 53
configurazione del driver 106
connessioni 54, 105
dispositivo 105
dispositivo di sicurezza I/O 56
esempio 55
moduli 53
moduli di comunicazione 18
moduli I/O standard 57
panoramica 53
parametri di rete 57
uso della connessione 54

F

file DNT 82, 83
finestra di dialogo New Controller 39
firma del task di sicurezza 92
  copia 103
  descrizione 14
  effetto sul download 108
  effetto sull'upload 107
  eliminazione 103
  generazione 102
  memorizzazione di un progetto 114
  operazioni non consentite 102
  restrizioni 103
  visualizzazione 119
Firmware Supervisor 118
forzatura 102

G

gateway 57
get system value (GSV)
  accessibilità 126
  definizione 11
  utilizzo 125

I

I/O
  codici di errore 134
  indicatore 120
  sostituzione modulo 44
I/O CIP Safety
  aggiunta 63
  autenticazione di configurazione 71
  dati di stato 74
  indirizzo di nodo 63
  monitoraggio dello stato 74
  reset ownership 72
incolla
  numero di rete di sicurezza 52
indicatore BAT 119
indicatori di stato 121, 129-130
  moduli I/O 74
indirizzo
  Dispositivo I/O di sicurezza Kinetix 73
indirizzo di nodo 63
indirizzo IP 57, 63
intervallo di pacchetto richiesto 93
  dati tag prodotto 89
  definizione 11
  I/O di sicurezza 67
  tag consumati 89
  tag consumato 97
Istruzioni Add-On 138
Istruzioni Add-on 19

K

kit di aggiornamento firmware 107, 118

L

limite del tempo di risposta
  I/O CIP Safety 67
limite del tempo di risposta della connessione 67, 97
Livelli prestazionali 11, 13
LOCK (blocco)
  vedere blocco di sicurezza.

M

Major Recoverable Fault
  messaggi 133
MajorFaultRecord 127
maschera di sottorete 57
massimo ritardo di rete osservato 68
  reset 97
memoria
  capacità 16
memoria non volatile 113-118
  scheda 114
memoria utente 16
memorizzazione di un progetto 114
messaggi
  errore 132
  stato di sicurezza 130
  stato generale 131
messaggi di stato generali 131
messaggio
  display di stato 131
modalità
  operativa 33
Modalità Esecuzione 33
modalità operativa 33
Modalità Programmazione 33
Modalità Remota 33, 34
modifica 102
module
  properties
    scheda Connection 72
moduli
  EtherNet/IP 53
modulo
  ControlNet 18
  DeviceNet 18
  EtherNet/IP 18
  indicatore di stato 74
modulo di alimentazione 24
  1756-ESMCAP 24
  autonomia 118
  definizione 11
  disinstallazione 34
  in carica 25, 37
  installazione 36
  memoria non volatile 116
modulo Guard I/O
  sostituzione 81-83
monitoraggio
  connessioni 120
  stato 74
multicast 11

N

network delay multiplier 69, 97
numero della rete di sicurezza
descrizione 13
gestione 47
numero di rete di sicurezza
assegnazione 47
assegnazione automatica 49
assegnazione manuale 49
basato sul tempo 48
copia 52
copia e incolla 52
definizione 11
impostazione 67
incolla 52
mancata corrispondenza 81
manuale 49
modifica 50
modifica del valore SNN del controllore 50
modifica del valore SNN dell'I/O 51
visualizzazione 41
numero di slot 40
numero seriale 106

O

oggetto di sicurezza
attributi 125

P

password
caratteri validi 43
impostazione 42
periodo task di sicurezza 68, 87, 93
probabilità di guasto all'ora (PFH)
definizione 11
probabilità di guasto su domanda (PFD)
definizione 11
produzione di un tag 95
produzione e consumo di tag 54, 58, 92
progetti di sicurezza
funzioni 19
programmazione 102
programmazione delle restrizioni 103
programmi di sicurezza 87
proprietà
configurazione 72
ripristino 72
proprietario della configurazione 71
identificazione 72
ripristino 72, 75
protezione dell'applicazione di sicurezza 100-103
blocco di sicurezza 100
firma del task di sicurezza 102
sicurezza 101
protezione della firma in modalità esecuzione 43
protezione modalità esecuzione 102, 103
protocollo di controllo ed informazioni
definizione 11

R

radiazione UV 23
reset
modulo 75
proprietà 72, 75
reset modulo 75
restrizioni
mappatura dei tag di sicurezza 98
programmazione 103
se è stata configurata una firma di sicurezza 102
se in blocco di sicurezza 100
software 103
rimozione e inserimento sotto tensione 22
RIUP
Vedere rimozione e inserimento sotto tensione (RIUP)
routine di errore del programma 125
routine di sicurezza 88
utilizzo di dati standard 98
RPI
vedere intervallo di pacchetto richiesto

S

SafetyTaskFaultRecord 127
salvataggio del programma
memoria non volatile 116
sblocco controllore 101
sblocco di sicurezza
controllore 101
icona 101
scariche elettrostatiche 23
scheda di memoria 113, 115, 118
installazione 26
rimozione 26
scheda Major Faults 123, 124
scheda Minor Faults 124
scheda Safety 101, 102, 122
autenticazione di configurazione 71
blocco di sicurezza 101
blocco di sicurezza del controllore 101
dati connessione 67
generazione di una firma del task di sicurezza 102
sblocco 101
sostituzione modulo 76
visualizzazione dello stato di sicurezza 107, 122
scheda SD
Vedere scheda Secure Digital.
scheda Secure Digital 24
installazione 28
rimozione 27
Vedere anche scheda di memoria.
selettore a chiave 16, 33
Servoazionamento Kinetix 5500 56
set system value (SSV)
accessibilità 126
utilizzo 125
simbolo di avviso 120
sincronizzazione temporale 45, 109

software
restrizioni 103
rete ControlNet 58
reti DeviceNet 60
USB 29
software ControlFLASH 31, 107, 115, 118
software RSLinx Classic
versione 18
software RSLogix 5000
restrizioni 103
Software RSNetWorx for DeviceNet
sostituzione modulo 81
sostituzione
configure always abilitata 80
configure only… enabled 76
modulo Guard I/O 75-83
stato
coprocessore di sicurezza 122
display 130-135
messaggi 130
messaggi di errore 132
messaggi, display 131
stato della rete
indicatore 74, 77, 79, 82
stato di sicurezza 13
effetto sul download 107
firma del task di sicurezza 102
programmazione delle restrizioni 103
pulsante 102, 120
visualizzazione 107, 119, 122

T

tag
accesso esterno 88, 92
alias 89
ambito 90
base 89
classe 91
constant value 92
consumato 89, 92
dati di sicurezza prodotti/consumati 90, 91
definiti nell'ambito del controllore 91
definiti nell'ambito del programma 91
denominazione 72
I/O di sicurezza 90, 91
panoramica 88
prodotto 89, 92
tipo 89
tipo di dati 90
vedere anche: tag di sicurezza.
tag alias 89
tag base 89
tag constant value 92
tag consumato 89, 92
tag definiti nell'ambito del controllore 91
tag definiti nell'ambito del programma 91
tag di sicurezza
creazione 88
definiti nell'ambito del controllore 91
definiti nell'ambito del programma 91
descrizione 88
mappatura 98-100
tipi di dati validi 90
tag prodotto 89, 92
task di sicurezza 86
esecuzione 87
priorità 86
tempo di watchdog 86
tempi di scansione
reset 103
tempo di risposta 87
tempo di sistema coordinato 109, 130
tempo di watchdog 86
terminologia 11
timeout multiplier 69, 97
tipi di dati
CONNECTION_STATUS 93
traduzione degli indirizzi di rete (NAT)
definizione 11
funzioni supportate 19
impostazione dell'indirizzo IP 65

U

unicast 11
connessioni 92, 95
upload
effetto del blocco di sicurezza 107
effetto della corrispondenza del controllore 106
effetto della firma del task di sicurezza 107
processo 110
USB
cavo 29, 105
connessione 29
driver 30
porta 29
software richiesto 29
tipo 29

V

versione firmware
aggiornamento 31, 32
corrispondenza 107
gestione 118
mancata corrispondenza 108, 109, 112
visualizzazione
stato di sicurezza 107

W

WallClockTime 116, 118
modulo di alimentazione 118
oggetto 37

X

XT
Vedere ambiente estremo.
vedere ambiente estremo.

Note:

Assistenza Rockwell Automation

Rockwell Automation fornisce informazioni tecniche in linea per assistere i clienti nell'utilizzo dei prodotti. Alla pagina http://www.rockwellautomation.com/support sono disponibili note tecniche e applicative, codici di esempio e collegamenti a service pack software. È inoltre possibile visitare il nostro Centro di assistenza all'indirizzo https://rockwellautomation.custhelp.com/ per trovare aggiornamenti software, chat e forum di supporto, informazioni tecniche e FAQ e per iscriversi agli aggiornamenti di notifica dei prodotti.

Offriamo inoltre vari programmi di supporto per l'installazione, la configurazione e la risoluzione dei problemi. Per ulteriori informazioni, contattare il distributore o il rappresentante Rockwell Automation di zona, oppure visitare il sito http://www.rockwellautomation.com/services/online-phone.

Assistenza all'installazione

Se si riscontra un problema entro le prime 24 ore dall'installazione, consultare le informazioni contenute nel presente manuale. È possibile contattare l'Assistenza clienti per ottenere l'assistenza iniziale necessaria per far funzionare il prodotto.

Stati Uniti o Canada	1.440.646.3434
Fuori dagli Stati Uniti o dal Canada	Utilizzare lo strumento Worldwide Locator all'indirizzo http://www.rockwellautomation.com/rockwellautomation/support/overview.page, oppure contattare il rappresentante Rockwell Automation di zona.

Restituzione di prodotti nuovi non funzionanti

Tutti i prodotti Rockwell Automation sono sottoposti a rigorosi collaudi per verificarne la piena funzionalità prima della spedizione dalla fabbrica. Tuttavia, qualora il prodotto presenti dei malfunzionamenti e debba essere restituito, seguire queste procedure.

Stati Uniti	Contattare il proprio distributore. Per completare la procedura di restituzione, è necessario fornire al proprio distributore un numero di pratica dell'Assistenza clienti (chiamare il numero telefonico indicato sopra per ottenerne uno).
Fuori dagli Stati Uniti	Per la procedura di restituzione, contattare il proprio rappresentante locale Rockwell Automation.

Feedback sulla documentazione

I vostri commenti ci consentono di soddisfare al meglio le vostre esigenze relative alla documentazione. Per qualsiasi suggerimento per migliorare il presente documento, compilare questo modulo, pubblicazione RA-DU002, disponibile all'indirizzo http://www.rockwellautomation.com/literature/.

Rockwell Automation pubblica le informazioni ambientali aggiornate relative al prodotto sul proprio sito Web all'indirizzo http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americhe: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496, USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Medio Oriente/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asia: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846

Italia: Rockwell Automation S.r.l., Via Gallarate 215, 20151 Milano, Tel: +39 02 334471, Fax: +39 02 33447701, www.rockwellautomation.it
Svizzera: Rockwell Automation AG, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Fax: 091 604 62 64, Customer Service: Tel: 0848 000 279

Pubblicazione 1756-UM022C-IT-P - Maggio 2015

© 2015 Rockwell Automation, Inc. Tutti i diritti riservati. Stampato negli USA.